This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(12) UK Patent Application (19) GB (11) 2 331 381 (13) A

(43) Date of A Publication 19.05.1999

(21) Application No 9811875.5

(22) Date of Filing 02.06.1998

(30) Priority Data
(31) 09314017 (32) 14.11.1997 (33) JP

(71) Applicant(s)
Fujitsu Limited
(Incorporated in Japan)
1-1 Kamikodanaka 4 -chome, Nakahara-ku,
Kawasaki-shi, Kanagawa 211-8588, Japan

(72) Inventor(s)
Jun Kamada
Yasutsugu Kuroda
Etsuo Ono

(74) Agent and/or Address for Service
Haseltine Lake & Co
Imperial House, 15-19 Kingsway, LONDON,
WC2B 6UD, United Kingdom

(51) INT CL[6]
G06F 1/00 12/14

(52) UK CL (Edition Q)
G4A AAP

(56) Documents Cited
GB 1588147 A EP 0281225 A2 WO 96/25700 A1
WO 95/16947 A1 US 5619571 A US 5610980 A
US 5555303 A US 5479509 A US 5050212 A

(58) Field of Search
UK CL (Edition P) G4A AAP
INT CL[6] G06F 1/00 12/14
Online: COMPUTER, EPODOC, WPI, PATENTS
CITATION INDEX

(54) Abstract Title

System for managing files, with alteration preventing/detecting function

(57) By storing an authenticator created from a data file in a secure area 31 usually inaccessible to a user, the alteration of the data file can be detected. Furthermore, by designating the data file as a main-file 33 and creating authenticators from various kinds of sub-files 34 related to the main-file, the size of the secure area where the authenticators are stored can be reduced. A computer 1 and storage unit 2 have reciprocal authentication units 11, 12.

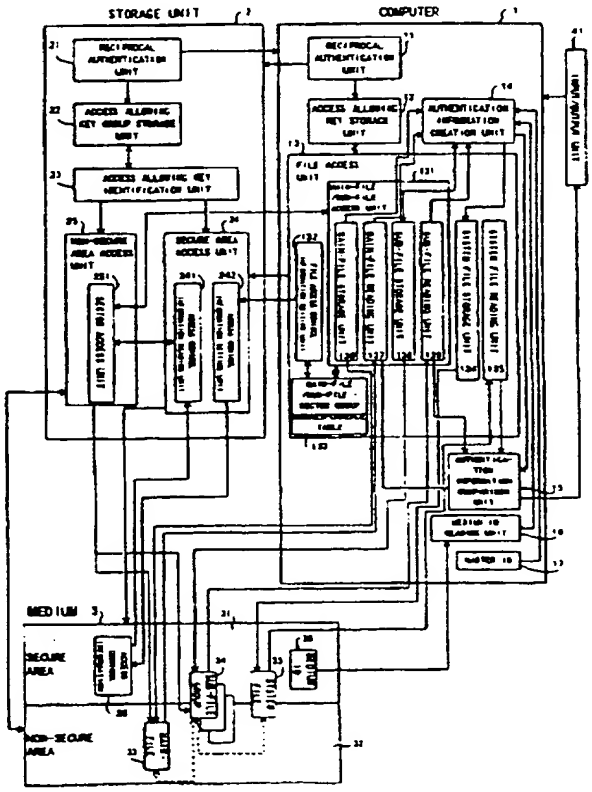

FIG. 1

GB 2 331 381 A

BNSDOCID: <GB___2331381A__I_>

SYSTEM FOR MANAGING FILES WITH ALTERATION PREVENTING/DETECTING FUNCTION

The present invention relates to a system for managing files having the functions of altering files and detecting the alteration of files, and more particularly to a file managing system for implementing the alteration prevention of files and detecting the alteration by storing authenticators indirectly created from files in an area inaccessible to the operator.

As the computerization of official documents such as tax-related slips, etc. is promoted, a demand for keeping computerized data as evidence, safely and for a long time, in the same way as data is preserved on paper, has been increasing. The computerized documents can be very easily processed and reused, and can easily be added to, deleted from, corrected or transferred via a network, etc. For this reason, the computerized data involves a risk of being altered by

BNSDOCID: <GB__2331381A__I_>
BNSDOCID: <GB_ 2331381A I >

a third party.

To solve this problem the applicant has applied for Japanese patent application No. 9-88485 ("File system and program storage medium" dated April 7, 1997). This is a file system in which illegal alteration by the low-level access of illegal users, or illegal and malicious alteration by authorized users can be detected by linking the file management module in the OS (operating system) with a storage medium (secure medium) where an area usually unaccessible to users (secure area) can be set and preserving authenticators for detecting the alteration of data files, the access logs of data files, etc. in the secure area relating the authenticators, the access logs, etc. to the data files.

However, in the above-mentioned conventional example, since access to a secure area by users is usually protected by a file system, in a system without such a file system, the secure area can be easily accessed, and as a result, authenticators, access logs, etc. related to data files can often be altered freely.

Although a necessary secure area differs in size, since the sizes of access logs, etc. expand dynamically, usually it is difficult to modify the

BNSDOCID <GB 2331381A I>

size of both a secure area and a normal area.

Embodiments of the present invention provide a system for managing files having alteration preventing/detecting functions for preventing a secure area from being easily accessed and preventing the authenticator and access log, etc. related to a data file from being freely altered, by means of reciprocal authentication obtained between a file system and a storing unit such as, for example, a unit of firmware.

Embodiments of the present invention provide a system for managing files having alteration preventing/detecting functions for dynamically modifying the size of both a secure area and a normal area by locating sub-files such as authenticators, access logs, etc. related to a data file being a main-file in the normal area, and locating only authenticators created from the sub-file in the secure area.

A system for managing files having alteration preventing/detecting functions may comprise a reciprocal authentication unit, an access allowing key storage unit, a file access unit, a main-file storage unit, a main-file reading

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

unit, a sub-file storage unit, a sub-file reading unit, a system file storage unit, a system file reading unit, an authentication information creation unit, an authentication information comparison unit, an access allowing key group storage unit, an access allowing key identification unit and a secure area access unit.

In the first aspect of the present invention the reciprocal authentication unit creates an access allowing key. The access allowing key storage unit stores the access allowing key. The file access unit sends out an access request together with the access allowing key. The access allowing key group storage unit stores all the access allowing keys. The access allowing identification unit identifies if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same. The secure area access unit accesses a secure area normally unaccessible.

In the second aspect of the present invention the sub-file storage unit stores files. The authentication information creation unit creates sub-file authentication information used to verify the sub-files. The system file storage unit stores the sub-

BNSDOCID <GB 2331381A I>

file authentication information relating the information to the main-file as a system file.

In the third aspect of the present invention the main-file storage unit stores a main-file. The authentication information creation unit creates main-file authentication information to be used to verify the main-file. The sub-file storage unit stores the main-file authentication information relating the information to the main-file as one of sub-files.

In the fourth aspect of the present invention the main-file storage unit stores a main-file. The authentication creation unit creates main-file authentication information to be used to verify the main-file. The sub-file storage unit stores the main-file authentication information relating the information to the main-file as one of sub-files. The sub-file storage unit stores one or a plurality of sub-files related to a main-file. The authentication information creation unit creates sub-file authentication information to be used to verify the sub-file. The system file storage unit stores the sub-file authentication information relating the information to the sub-file as a system file.

In the fifth aspect of the present invention the sub-file reading unit reads sub-files. The

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB 2331381A I >

authentication information creation unit creates sub-file authentication information from sub-files read from the sub-file reading unit. The system file reading unit reads sub-file authentication information from a system file related to the sub-file. The authentication information comparison unit compares the sub-file authentication information created by the authentication information creation unit with the sub-file authentication information read by the system file reading unit.

In the sixth aspect of the present invention the main-file reading unit reads a main-file. The authentication information creation unit creates main-file authentication information from a main-file read from the main-file reading unit. The sub-file reading unit reads main-file authentication information from sub-files related to the main-file. The authentication information comparison unit compares the main-file authentication information created by the authentication information creation unit with the main-file authentication information read by the sub-file reading unit.

In the seventh aspect of the present invention the main-file reading unit reads a main-file. The sub-file reading unit reads one or a plurality of sub-

BNSDOCID: <GB 2331381A_I_>

files related to the main-file and the main-file authentication information from sub-files related to the main-file. The system file reading unit reads sub-file authentication information from a system file related to the sub-file. The authentication information creation unit creates main-file authentication information from a main-file read by the main-file reading unit, and creates sub-file authentication information from sub-files read by the sub-file reading unit. The authentication information comparison unit compares the main-file authentication information created by the authentication information creation unit with the main-file authentication information read by the sub-file reading unit, and compares the sub-file authentication information created by the authentication information creation unit with the sub-file authentication information read by the system file reading unit.

The present invention will be more apparent from the following detailed description in conjunction with the accompanying drawings, in which:

Fig.1 shows an entire configuration of a file management system having alteration

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

preventing/detecting functions of the present invention.

Fig.2 explains a file composition of the present invention.

Fig.3 explains a calculation method of a message authentication code (MAC) process.

Fig.4 shows a configuration of a file management system having alteration preventing/detecting functions of the first embodiment of this invention.

Fig.5 is a flowchart showing an operation of the first embodiment of this invention.

Fig.6 shows a configuration of a file management system having alteration preventing/detecting functions of the second embodiment of this invention.

Fig.7 is a flowchart showing an operation of the second embodiment of this invention.

Fig.8 shows a configuration of a file management system having alteration preventing/detecting functions of the third embodiment of this invention.

Fig.9 is a flowchart showing an operation of the third embodiment of this invention.

Fig.10 shows a configuration of a file management system having alteration preventing/detecting functions of the fourth embodiment of this invention.

Fig.11 is a flowchart showing an operation of

BNSDOCID: <GB 2331381A_I_>

the fourth embodiment of this invention.

Fig.12 shows a configuration of a file management system having alteration preventing/detecting functions of the fifth embodiment of this invention.

Fig.13 is a flowchart showing an operation of the fifth embodiment of this invention.

Fig.14 shows a configuration of a file management system having alteration preventing/detecting functions of the sixth embodiment of this invention.

Fig.15 shows a configuration of a file management system having alteration preventing/detecting functions of the seventh embodiment of this invention.

Fig.16 shows a configuration of a file management system having alteration preventing/detecting functions of the eighth embodiment of this invention.

Fig.17 is a flowchart showing an operation of the eighth embodiment of this invention.

Fig.18 shows a configuration of a file management system having alteration preventing/detecting functions of the ninth embodiment of this invention.

Fig.19 is a flowchart showing an operation of the ninth embodiment of this invention.

Fig.20 shows a configuration of a file management system having alteration preventing/detecting

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

functions of the tenth embodiment of this invention.

Fig.21 is a flowchart showing an operation of the tenth embodiment of this invention.

Fig.22 shows a configuration of a file management system having alteration preventing/detecting functions of the eleventh embodiment of this invention.

Fig.23 is a flowchart showing an operation of the eleventh embodiment of this invention.

Fig.24 shows a configuration of a file management system having alteration preventing/detecting functions of the twelfth embodiment of this invention.

Fig.25 shows a configuration of a file management system having alteration preventing/detecting functions of the thirteenth embodiment of this invention.

Fig.26 shows a configuration of a file management system having alteration preventing/detecting functions of the fourteenth embodiment of this invention.

Fig.27 is a flowchart showing an operation of the fourteenth embodiment of this invention.

Fig.28 shows a configuration of a file management system having alteration preventing/detecting functions of the fifteenth embodiment of this

BNSDOCID <GB 2331381A_I_>

invention.

Fig.29 is a flowchart showing an operation of the fifteenth embodiment of this invention.

Fig.30 shows a configuration of a file management system having alteration preventing/detecting functions of the sixteenth embodiment of this invention.

Fig.31 shows a configuration of an alteration preventing/detecting system.

The embodiments of this invention are described in detail below with reference to the drawings.

The invention of claim 1 is a file system comprising a computer and a storage unit. The computer comprises a reciprocal authentication unit for reciprocally authenticating the computer with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for reciprocally authenticating the storage unit with the computer and

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible.

The invention of claim 2 is the file management system according to claim 1, wherein both the authentication unit of the computer and file access unit are implemented by a unit of hardware.

The invention of claim 3 is a file management system comprising a sub-file storage unit for storing one or a plurality of sub-files related to a main-file, an authentication information creation unit for creating sub-file authentication information to be used to verify the sub-files, and a system file storage unit for storing the sub-file authentication information relating the information to the sub-file as a system file.

The invention of claim 4 is a file management system comprising a main-file storage unit for storing

BNSDOCID <GB 2331381A_I_>

a main-file, an authentication information creation unit for creating main-file authentication information to be used to verify the main-file, and a sub-file storage unit for storing one of sub-files to which the main-file authentication information is related.

The invention of claim 5 is a file management system comprising a main-file storage unit for storing a main-file, an authentication information creation unit for creating main-file authentication information to be used to verify the main-file, a sub-file storage unit for storing one of sub-files to which the main-file authentication information is related, a sub-file storage unit for storing one or a plurality of sub-files related to a main-file, an authentication information creation unit for creating sub-file authentication information to be used to verify the sub-file, and a system file storage unit for storing the sub-file authentication information relating the information to the sub-file as a system file.

The invention of claim 6 is a file management system according to claim 5, wherein the main-file, sub-files and system file are stored in a non-secure area usually accessible.

The invention of claim 7 is a file management system according to claim 5, wherein the main-file,

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

and the sub-files and system file are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

The invention of claim 8 is a file management system according to claim 5, wherein the main-file and sub-files, and the system file are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

The invention of claim 9 is a file management system according to claim 6, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access

BNSDOCID <GB 2331381A_I_>

allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible, and the authentication information creation unit reads a medium ID peculiar to a medium stored in the secure area after reciprocally authenticating the computer and storage unit and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 10 is a file management system according to claim 7, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access

BNSDOCID: <GB 2331381A I>
BNSDOCID: <GB 2331381A I>

allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible. The authentication information creation unit reads a medium ID peculiar to a medium stored in the secure area after reciprocally authenticating the computer and storage unit and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 11 is a file management system according to claim 8, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for

BNSDOCID <GB 2331381A_I_>

reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible. The authentication information creation unit reads a medium ID peculiar to a medium stored in the secure area after reciprocally authenticating the computer and storage unit, and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 12 is a file management system according to claim 9, wherein the reciprocal authentication information unit of the computer and the file access unit are implemented by means of hardware.

The invention of claim 13 is a file management system according to claim 9, wherein the medium ID is a card ID.

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB 2331381A _I_>

The invention of claim 14 is a file management system according to claim 9, wherein the medium ID is a master ID.

The invention of claim 15 is a file management system according to claim 9, wherein the authentication information is created for each record of a file.

The invention of claim 16 is a file management system according to claim 10, wherein the authentication information is created for each record of a file.

The invention of claim 17 is a file management system according to claim 11, wherein the authentication information is created for each record of a file.

The invention of claim 18 is a file management system comprising a sub-file reading unit for reading one or a plurality of sub-files related to a main-file, an authentication information creation unit for creating sub-file authentication information from sub-files read by the sub-file reading unit, a system file reading unit for reading sub-file authentication information from a system file related to the sub-file, and an authentication information comparison unit for comparing the sub-file authentication

BNSDOCID: <GB 2331381A_I_>

information created by the authentication information creation unit with the sub-file authentication information read by the system file reading unit.

The invention of claim 19 is a file management system comprising a main-file reading unit for reading a main-file, an authentication information creation unit for creating main-file authentication information from a main-file read by the main-file reading unit, a sub-file reading unit for reading main-file authentication information from sub-files related to the main-file, and an authentication information comparison unit for comparing the main-file authentication information created by the authentication information creation unit with the main-file authentication information read by the sub-file reading unit.

The invention of claim 20 is a file management system comprising a main-file reading unit for reading a main-file, a sub-file reading unit for reading main-file authentication information from one or a plurality of sub-files related to the main-file and sub-files related to the main-file, a system file reading unit for reading sub-file authentication information from a system file related to the sub-file, an authentication information creation unit for

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB__2331381A_I_>

creating main-file authentication information from a main-file read by the main-file reading unit and creating sub-file authentication information from sub-files read from the sub-file reading unit, an authentication information comparison unit for comparing the main-file authentication information created by the authentication information creation unit with the main-file authentication information read by the sub-file reading unit and comparing the sub-file authentication information created by the authentication information creation unit with the sub-file authentication information read by the system file reading unit.

The invention of claim 21 is a file management system according to claim 20, wherein the main-file, sub-files and system file are stored in a non-secure area usually accessible.

The invention of claim 22 is a file management system according to claim 20, wherein the main-file, and the sub-files and system file are stored in a non-secure area usually accessible and a secure area usually unaccessible, respectively.

The invention of claim 23 is a file management system according to claim 20, wherein the main-file and sub-files, and the system file are stored in a

BNSDOCID <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

non-secure area usually accessible and a secure area usually unaccessible, respectively.

The invention of claim 24 is a file management system according to claim 21, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible. The authentication information creation unit reads a medium ID peculiar

BNSDOCID <GB__2331381A_I_>
BNSDOCID: <GB__2331381A_I_>

to a medium stored in the secure area after reciprocally authenticating the computer and storage unit, and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 25 is a file management system according to claim 22, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key and a file access unit for sending an access request together with the access allowing key, the storage unit comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the

BNSDOCID <GB___2331381A_I_>
BNSDOCID: <GB 2331381A I >

same, and a secure area access unit for accessing a secure area usually unaccessible. The authentication information creation unit reads a medium ID peculiar to a medium stored in the secure area after reciprocally authenticating the computer and storage unit and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 26 is a file management system according to claim 23, comprising a computer and a storage unit, wherein the computer comprises a reciprocal authentication unit for reciprocally authenticating with the storage unit and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key storage unit for storing the access allowing key, and a file access unit for sending an access request together with the access allowing key. The storage unit comprises a reciprocal authentication unit for reciprocally authenticating with the computer and creating an access allowing key when the computer and storage unit are reciprocally authenticated, an access allowing key group storage unit for storing all the access allowing keys, an access allowing key identification unit for identifying if the access

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

allowing key stored in the access allowing key storage unit and at least one access allowing key stored in the access allowing key group storage unit, are the same, and a secure area access unit for accessing a secure area usually unaccessible. The authentication information creation unit reads a medium ID peculiar to a medium stored in the secure area after reciprocally authenticating the computer and storage unit, and uses the medium ID to create both the main-file authentication information and sub-file authentication information.

The invention of claim 27 is a file management system according to claim 24, wherein the reciprocal authentication unit of the computer and the file access unit are implemented by means of hardware.

The invention of claim 28 is a file management system according to claim 24, wherein the medium ID is a card ID.

The invention of claim 29 is a file management system according to claim 24, wherein the medium ID is a master ID.

The invention of claim 30 is a file management system according to claim 24, wherein the authentication information is created for each record of a file.

BNSDOCID <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

The invention of claim 31 is a file management system according to claim 1, wherein the storage unit comprises a sector access unit for accessing a main-file or sub-files related to the main-file in units of sectors or sector groups, and the secure area access unit comprises an access control information reading unit for reading access control information stored in the secure area.

The invention of claim 32 is a file management system according to claim 31, wherein the secure area access unit further comprises an access control information setting unit for setting access control information in the secure area.

The invention of claim 33 is a file management system according to claim 9, wherein authentication information is created using one, two or all of the medium ID, card ID and master ID.

The invention of claim 34 is a file management system according to claim 24, wherein authentication information is created using one, two or all of the medium ID, card ID and master ID.

The invention of claim 35 is a file management method comprising the reciprocal authentication step of creating an access allowing key, the access allowing key storing step of storing the access

BNSDOCID: <GB __2331381A__I_>
BNSDOCID: <GB .. 2331381A_I >>

allowing keys, the file access step of sending an access request together with the access allowing key, the access allowing key group storing step of storing all the access allowing keys, the access allowing key identifying step of identifying if the access allowing key stored in the access allowing key storing step and at least one access allowing key stored in the access allowing key group storing step, are the same, and the secure area accessing step of accessing a secure area usually unaccessible when reciprocal authentication is carried out between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated.

The invention of claim 36 is a computer readable storage medium with a recorded file management program for enabling a computer to implement the reciprocal authentication step of creating an access allowing key, the access allowing key storing step of storing the access allowing key, the file access step of sending an access request together with the access allowing key, the access allowing key group storing step of storing all the access allowing keys, the access allowing key identifying step of identifying if the access allowing key stored in the access allowing key storing step and at least one access

BNSDOCID: <GB 2331381A_I_>

allowing key stored in the access allowing key group storing step, are the same, and the secure area accessing step of accessing a secure area usually unaccessible when reciprocal authentication is carried out between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated.

Fig.1 shows the entire configuration of the file management system having the alteration preventing/detecting functions of the present invention.

Each component unit is described later with reference to Figs. 4, 6, 8, 10, 12, 14, 15, 16, 18, 20, 22, 24, 25, 26, 28 and 30 while describing each embodiment of this invention.

Each component unit on a computer 1 side such as a reciprocal authentication unit 11, authentication information creation unit 14 and authentication information comparison unit 15, etc., can be a software subroutine of a file management module in an OS, or can be constructed by means of hardware.

Fig.2 explains the file composition of the present invention.

Authenticators created from a main-file are stored in sub-files, and authenticators created from

BNSDOCID <GB_ 2331381A_I_>
BNSDOCID: <GB_ 2331381A I >

sub-files are stored in a system file.

Fig.3 explains the calculation method of a message authentication code (MAC) processing.

Source data such as a main-file, sub-files, etc. are divided, for example, into several blocks of 64 bits, and are ciphered. The exclusive-ORs of the ciphered value and the next 64 bits are calculated, and are also ciphered. Although each ciphered value or a part of the value, for example, the higher-order 32 bits, can be made an authenticator, in each embodiment of this invention described later, this process is repeated to the last block of the source data, and higher-order 32 bits finally obtained shall be an authenticator.

Fig.4 shows the configuration of the file management system having the alteration preventing/detecting functions of the first embodiment of this invention. Fig.5 is a flowchart showing the operation of the first embodiment of this invention.

In step S51 the reciprocal authentication unit 11 on the computer 1 side and the reciprocal authentication unit 21 on the storage unit 2 side are reciprocally authenticated. If in step S52 the reciprocal authentication succeeds, in step S53 a common access allowing key is created. In step S54 the

BNSDOCID <GB 2331381A I>

reciprocal authentication unit 11 on the computer 1 side transfers the created allowing key to an access allowing key storage unit 12, and the key is stored in the storage unit 12. The reciprocal authentication unit 21 on the storage unit 2 side also transfers the created allowing key to an access allowing key storage unit 22, and the key is stored in the storage unit 22. The reciprocal authentication method shall use, for example, a general open key.

In step S55, when accessing a secure area 31 in a medium 3 to be accessed via the storage unit 2, a file access unit 13 sends the access allowing key to a secure area access unit 24 of the storage unit 2 together with an access request.

In step S56 an access allowing key identification unit 23 judges whether or not there is the same access allowing key as the access allowing key sent from the file access unit 13 to the secure area access unit 24 together with the access request, in the access allowing key storage unit 22. If there is the same access allowing key, in step S57 the secure area access unit 24 accesses a secure area 31.

Each of the reciprocal authentication unit 11 and file access unit 13 on the computer side 1 can be a software subroutine of a file management module in an

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

OS or can be constructed by means of hardware.

Fig.6 shows the configuration of the file management system having the alteration preventing/detecting functions of the second embodiment of this invention. Fig.7 is a flowchart showing the operation of the second embodiment of this invention.

In step S71 a sub-file storage unit 138 stores sub-files 34 in the medium 3 in units of blocks, if there is still another sub-file 34 to be processed when the flow returns from the process in step S74, described later, the sub-file storage unit 138 reads the sub-file 34, and combines the sub-file 34 with the already stored sub-files 34, and transfers the combined sub-file to an authentication information creation unit 14.

In step S72 the authentication information creation unit 14 creates an authenticator being authentication information from the combined sub-file, which is transferred to a system file storage unit 134. In step S73 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S71, where the next block of the sub-file 34 is processed.

BNSDOCID: <GB 2331381A I>
BNSDOCID: <GB 2331381A I>

In step S73 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S71, where the next sub-file 34 is processed.

In step S74 the system file storage unit 134 makes a set of an arbitrary ID for exclusively identifying both a main-file 33 and a sub-file group 34, and an authenticator being authentication information, and stores the set in a system file 35.

Fig.8 shows the configuration of the file management system having the alteration preventing/detecting functions of the third embodiment of this invention. Fig.9 is a flowchart showing the operation of the third embodiment of this invention.

In step S91 a main-file storage unit 136 stores the main-file 33 in the medium 3 in units of blocks, and also transfers the main-file 33 to the authentication information creation unit 14.

In step S92, when receiving this main-file 33, the authentication information creation unit 14 creates an authenticator being authentication information, and transfers the authenticator to the sub-file storage unit 138. In step S93 it is checked whether or not all the blocks of the main-file 33

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB_ _2331381A_I_>

are processed. If there is still another block to be processed, the flow returns to step S91, where the next block of the main-file 33 is processed.

In step S94 the sub-file storage unit 138 makes a set of an arbitrary ID for exclusively identifying a main-file 33 and an authenticator being authentication information, and stores the set in a specific sub-file 34.

Fig.10 shows the configuration of the file management system having the alteration preventing/detecting functions of the fourth embodiment of this invention. Fig.11 is a flowchart showing the operation of the fourth embodiment of this invention.

In step S111 the main-file storage unit 136 stores the main-file 33 in the medium 3 in units of blocks, and transfers the main-file 33 to the authentication information creation unit 14.

In step S112 the authentication information creation unit 14 creates an authenticator being authentication information from the main-file 33, and transfers the authenticator to the sub-file storage unit 138. In step S113 it is checked whether or not all the blocks of the main-file 33 are processed. If there is still another block to be processed, the flow

BNSDOCID: <GB 2331381A I>
BNSDOCID: <GB 2331381A I>

returns to step S111, where the next block of the main-file 33 is processed.

In step S114 the sub-file storage unit 138 makes a set of an arbitrary ID for exclusively identifying a main-file 33 and an authenticator being authentication information, and stores the authenticator in a specific sub-file 34.

Then, in step S115 a sub-file reading unit 139 reads the sub-file group 34, and transfers the sub-file group 34 to the authentication information creation unit 14.

In step S116 the authentication information creation unit 14 creates an authenticator being authentication information, and transfers the authenticator to the system file storage unit 134. In step S117 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S115, where the next block of the sub-file 34 is processed.

In step S118 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S115, where the next sub-file 34 is processed. By executing this process on all of the

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB__ 2331381A I >

sub-files, the sub-file reading unit 139 is able to read all of the sub-files in the sub-file group 34, and is able to transfer all of the sub-files in the sub-file group 34 to the authentication information creation unit 14.

In step S119 the system file storage unit 134 makes a set of an arbitrary ID for exclusively identifying both main-file 33 and sub-file group 34, and an authenticator being authentication information, and stores the set in the system file 35.

Although the main-file 33 is stored in a non-secure area 32, the sub-files 34 and system file 35 can be stored in either the secure area 31 or the non-secure area 32.

That is, the main-file 33 being actual data has to be stored in the non-secure area 32, and since the sub-files 34 and system file 35 are not directly required to be accessed nor are directly accessed, the sub-files 34 and system file 35 can be stored in either the secure area 31 or the non-secure area 32.

Fig.12 shows the configuration of the file management system having the alteration preventing/detecting functions of the fifth embodiment of this invention. Fig.13 is a flowchart showing the operation of the fifth embodiment of this invention.

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I>

The reciprocal authentication described in the first embodiment of this invention is carried out in advance.

In step S130 a medium ID reading unit 16 reads a medium ID 36 from the secure area 31 in the medium 3, and transfers the medium ID 36 to the authentication information creation unit 14.

In step S131 the main-file storage unit 136 stores the main-file 33 in the medium 3 in units of blocks, and also transfers the main-file 33 to the authentication information creation unit 14.

In step S132, when receiving the main-file 33, the authentication information creation unit 14 creates an authenticator being authentication information from the main-file 33 using the medium ID 36 as a key, and transfers the authenticator to the sub-file storage unit 138. It is assumed here that the authenticator is created using a data encryption standard-message authentication code (DES-MAC).

In step S133 it is checked whether or not all the blocks of the main-file 33 are processed. If there is still another block to be processed, the flow returns to step S131, and the next block of the main-file 33 is processed.

In step S134 the sub-file storage unit 138 makes

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB__ 2331381A_I_>

a set of an arbitrary ID for exclusively identifying a main-file 33 and an authenticator being authentication information, and stores the set in a specific sub-file 34.

Then, in step S135 a sub-file reading unit 139 reads sub-files, and transfers the sub-files to the authentication information creation unit 14. Furthermore, when the flow returns from the process in step S138, described later, the sub-file reading unit 139 combines the data stored in step S134, and transfers the data to the authentication information creation unit 14. That is, the sub-file reading unit 139 reads all of the sub-file group 34, combines all of the stored sub-file group 34, and transfers the sub-file group 34 to the authentication information creation unit 14.

In step S136 the authentication information creation unit 14 creates an authenticator being authentication information in the same way as described above, and transfers the authenticator to the system file storage unit 134.

In step S137 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S135, where the next block of the sub-file 34

BNSDOCID: <GB 2331381A I >
BNSDOCID: <GB 2331381A I >

is processed.

In step S138 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S135, where the next sub-file 34 is processed.

In step S139 the system file storage unit 134 makes a set of an arbitrary ID for exclusively identifying both the main-file 33 and sub-files 34, and authentication information, and stores the set in the system file 35.

The medium ID 36 used as a key when creating the authenticator can also be read from the medium 3 in advance.

Furthermore, the above-mentioned process can also be executed for each record composing the file of the main-file 33 and sub-files 34.

Fig.14 shows the configuration of the file management system having the alteration preventing/detecting functions of the sixth embodiment of this invention.

The configuration and basic operation of the sixth embodiment of this invention are the same as the configuration and basic operation of the fifth embodiment of this invention, except that the medium

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

ID 36 read by the medium ID reading unit 16 in the fifth embodiment of this invention described with reference to Fig.12, is replaced with a card ID 18 in the sixth embodiment of this invention.

Fig.15 shows the configuration of the file management system having the alteration preventing/detecting functions of the seventh embodiment of this invention.

The configuration and basic operation of the seventh embodiment of this invention are the same as the configuration and basic operation of the fifth embodiment of this invention, except that the medium ID 36 read by the medium ID reading unit 16 in the fifth embodiment of this invention described with reference to Fig.12 is replaced with a master ID 17 in the seventh embodiment of this invention.

Fig.16 shows the configuration of the file management system having the alteration preventing/detecting functions of the eighth embodiment of this invention. Fig.17 is a flowchart showing the operation of the eighth embodiment of this invention.

In step S171, when a verification request is issued by a higher-order layer (a user, etc.) via input/output unit 41, the system file reading unit 135

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A_I_>

reads an authenticator being corresponding authentication information from the system file 35, and transfers the authenticator to an authentication information comparison unit 15.

On the other hand, in step S172 the sub-file reading unit 139 reads the sub-files 34 in units of blocks, and transfers the sub-files 34 to the authentication information creation unit 14.

In step S173 the authentication information creation unit 14 creates an authenticator being authentication information, and transfers the authenticator to the authentication information comparison unit 15.

In step S174 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S172, where the next block of the sub-file 34 is processed.

In step S175 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S172, where the next sub-file 34 is processed.

In step S176 the authentication information comparison unit 15 compares these authenticators being

BNSDOCID <GB__2331381A_I_>
BNSDOCID: <GB_ 2331381A_I_>

authentication information. If the authenticators are the same, the authentication information comparison unit 15 reports the successful verification to the higher-order layer. If the authenticators are different, the authentication information comparison unit 15 reports the failed verification to the higher-order layer.

Fig.18 shows the configuration of the file management system having the alteration preventing/detecting functions of the ninth embodiment of this invention. Fig.19 is a flowchart showing the operation of the ninth embodiment of this invention.

In step S191, when a verification request is issued by a higher-order layer (a user, etc.) via input/output unit 41, the sub-file reading unit 139 reads an authenticator being corresponding authentication information from the specific file 34, and transfers the authenticator to an authentication information comparison unit 15.

On the other hand, in step S192 the main-file reading unit 137 reads a main-file 33 in units of blocks, and transfers the main-file 33 to the authentication information creation unit 14.

In step S193 the authentication information creation unit 14 creates an authenticator being

BNSDOCID <GB 2331381A_1_>
BNSDOCID: <GB 2331381A 1 >

authentication information, and transfers the authenticator to the authentication information comparison unit 15.

In step S194 it is checked whether or not all the blocks of the main-file 33 are processed. If there is still another block to be processed, the flow returns to step S192, where the next block of the main-file 33 is processed.

In step S195 the authentication information comparison unit 15 compares these authenticators being authentication information. If the authenticators are the same, the authentication information comparison unit 15 reports the successful verification to the higher-order layer. If the authenticators are different, the authentication information comparison unit 15 reports the failed verification to the higher-order layer.

Fig.20 shows the configuration of the file management system having the alteration preventing/detecting functions of the tenth embodiment of this invention. Fig.21 is a flowchart showing the operation of the tenth embodiment of this invention.

In step S210, when a reading request for reading a main-file 33 is issued, first the system file reading unit 135 reads an authenticator being

BNSDOCID <GB__2331381A__I_>
BNSDOCID: <GB 2331381A I >

corresponding authentication information from the system file 35, and transfers the authenticator to the authentication information comparison unit 15.

On the other hand, in step S211 the sub-file reading unit 139 reads sub-files 34 in units of blocks, and transfers the sub-files to the authentication information creation unit 14.

In step S212 the authentication information creation unit 14 creates an authenticator being authentication information from these sub-files in units of blocks, and transfers the authenticator to the authentication information comparison unit 15.

In step S213 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S211, where the next block of the sub-file 34 is processed.

In step S214 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S211, where the next sub-file 34 is processed.

In step S215 the authentication information comparison unit 15 compares the authenticator being the read authentication information with the

BNSDOCID <GB___2331381A_I_>
BNSDOCID: <GB 2331381A I >

authenticator being created authentication information, and if the authenticators are different, reports the failed verification to the higher-order layer.

Then, if the verification succeeds, in step S216 the sub-file reading unit 139 reads an authenticator being the authentication information for the main-file 33 from the sub-files 34, and transfers the authenticator to the authentication information comparison unit 15.

On the other hand, in step S217 the main-file reading unit 137 reads the main-file 33 in units of blocks, and transfers the main-file 33 to the authentication information creation unit 14.

In step S218 the authentication information creation unit 14 creates an authenticator being authentication information in units of blocks, and transfers the authenticator to the authentication information comparison unit 15.

In step S219 it is checked whether or not all the blocks of the main-file 33 are processed. If there is still another block to be processed, the flow returns to step S217, and the next block of the main-file 33 is processed.

In step S220 the authentication information

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

comparison unit 15 compares the authenticator being read authentication information with the authenticator being created authentication information, and reports the result of the verification to the higher-order layer.

Although the main-file 33 is stored in a non-secure area, the sub-files 34 and system file 35 can be stored in either the secure area or the non-secure area.

Fig.22 shows the configuration of the file management system having the alteration preventing/detecting functions of the eleventh embodiment of this invention. Fig.23 is a flowchart showing the operation of the eleventh embodiment of this invention.

When a verification request is issued by a higher-order layer (a user, etc.) via the input/output unit 41, in step S230 the medium ID reading unit 16 reads a medium ID 36 from the secure area 31 in the medium 3, and transfers the medium ID 36 to the authentication information creation unit 14.

In step S231 the system file reading unit 135 reads an authenticator being corresponding authentication information from the system file 35, and transfers the authenticator to the authentication

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

information comparison unit 15.

In step S232 the sub-file reading unit 139 reads sub-files 34 in units of blocks, and transfers the sub-files to the authentication information creation unit 14.

In step S233 the authentication information creation unit 14 creates an authenticator being authentication information using the medium ID 36 as a key, and transfers the authenticator to the authentication information comparison unit 15.

In step S234 it is checked whether or not all the blocks of the sub-file 34 are processed. If there is still another block to be processed, the flow returns to step S232, where the next block of the sub-file 34 is processed.

In step S235 it is checked whether or not all the plurality of sub-files 34 are processed. If there is still another sub-file 34 to be processed, the flow returns to step S232, where the next sub-file 34 is processed.

In step S236 the authentication information comparison unit 15 compares the authenticator being the read authentication information with the authenticator being the created authentication information, and reports the failed verification to

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A_I_>

the higher order layer if the authenticators are not the same.

Then, if the verification succeeds, in step S237 the sub-file reading unit 139 reads an authenticator being authentication information from a specific sub-file 34, and transfers the authenticator to the authentication information comparison unit 15.

In step S238 the main-file reading unit 137 reads a main-file 33 in units of blocks, and transfers the main-file 33 to the authentication information creation unit 14.

In step S239 the authentication information creation unit 14 creates an authenticator being authentication information in units of blocks using the medium ID 36 as a key, and transfers the authenticator to the authentication information comparison unit 15.

In step S240 it is checked whether or not all the blocks of the main-file 33 are processed. If there is still another block to be processed, the flow returns to step S238, and the next block of the main-file 33 is processed.

In step S241 the authentication information comparison unit 15 compares the authenticator being the read authentication information with the

BNSDOCID: <GB 2331381A I >
BNSDOCID: <GB 2331381A I >

authenticator being the created authentication information. If the authenticators are the same, the authentication information comparison unit 15 reports the successful verification to the higher order layer. If the authenticators are different, the authentication information comparison unit 15 reports the failed verification to the higher order layer.

The medium ID 36 to be used as a key when creating an authenticator can also be read from the medium 3 in advance.

Furthermore, the above-mentioned process can be executed for each record composing both the main-file 33 and sub-files 34.

Fig.24 shows the configuration of the file management system having the alteration preventing/detecting functions of the twelfth embodiment of this invention.

The configuration and basic operation of the twelfth embodiment of this invention are the same as the configuration and basic operation of the eleventh embodiment of this invention, except that the medium ID 36 read by the medium ID reading unit 16 in the eleventh embodiment of this invention described with reference to Fig.22 is replaced with a card ID 18 in the twelfth embodiment of this invention.

BNSDOCID <GB__2331381A__I_>
BNSDOCID: <GB__2331381A_I_>

Fig.25 shows the configuration of the file management system having the alteration preventing/detecting functions of the thirteenth embodiment of this invention.

The configuration and basic operation of the thirteenth embodiment of this invention are the same as the configuration and basic operation of the eleventh embodiment of this invention, except that the medium ID 36 read by the medium ID reading unit 16 in the eleventh embodiment of this invention described with reference to Fig.22 is replaced with a master ID 17 common to a plurality of pieces of hardware in the twelfth embodiment of this invention.

Fig.26 shows the configuration of the file management system having the alteration preventing/detecting functions of the fourteenth embodiment of this invention. Fig.27 is a flowchart showing the operation of the fourteenth embodiment of this invention.

In step S271 an access control information setting unit 242 sets and updates the setting of access control information 38. Various items are considered as a setting policy at the time of setting, for example, "once set to be unable to write, a sector shall never be set able to write again" can be

BNSDOCID <GB 2331381A I>

considered.

In step S272 the access control information reading unit 241 reads the access control information 38 in the secure area 31, and if the access is not allowed, reports the refusal to the user.

If the access is allowed, in step S273 a sector access unit 251 receives an access (reading/writing) request, and accesses a sector (group) composed of the main-file 33 and sub-files 34 in the non-secure area 32 of the storage medium 3.

Fig.28 shows the configuration of the file management system having the alteration preventing/detecting functions of the fifteenth embodiment of this invention. Fig.29 is a flowchart showing the operation of the fifteenth embodiment of this invention.

In step S291 an access control information setting unit 132 converts files designated by a higher-order layer to a sector list using a main-file/ sub-file - sector group correspondence table 133, and sends the sector list to the access control information setting unit 242 in the storage unit 2 together with an access mode such as read only/ write only/ read and write, etc.

In step S292 the access control information

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

setting unit 242 in the storage unit 2 sets and updates the setting of the access control information 38 stored in the medium 3 according to the setting policy. As the setting policy in this case, for example, "once set to be unable to write, a sector shall be never set to be able to write again" is considered.

In step S293 a main-file/sub-file access unit 131 converts both main-file 33 and sub-files 34 to be accessed to a sector (group) according to the main-file/sub-file - sector group correspondence table 133, and issues a request to a sector access unit 251.

In step S294 the sector access unit 251 executes or refuses the sector access according to the access control information 38 read by the access control information reading unit 241.

Fig.30 shows the configuration of the file management system having the alteration preventing/detecting functions of the sixteenth embodiment of this invention.

An arbitrary combination consisting of one, two or all of the medium ID 36, card ID 18 and master ID 17 in the fifth embodiment described with reference to Fig.12, the sixth embodiment described with reference to Fig.14, the seventh embodiment described

BNSDOCID <GB 2331381A_I_>

with reference to Fig.15, the eleventh embodiment described with reference to Fig.22, the twelfth embodiment described with reference to Fig.24 and the thirteenth embodiment described with reference to Fig.25, can also be used.

In this case, for example, it is assumed that information for indicating a lot number is put in a part of the medium ID 36, and the specific lot is made from a material suited for long time preservation or is carefully surface-checked.

Since official documents have to be preserved for a long time, a file system reads the medium ID 36 when inserting a medium, and if the medium is not included in the above-mentioned special lot, reports to the user that the medium cannot be used.

It is needless to say that only if the functions of the present invention are to be executed, the present invention can be applied to a single apparatus, a system or integrated apparatus consisting of a plurality of apparatuses or a system in which the process can be executed via a network such as a LAN, etc.

As shown in Fig.31 the present invention can be implemented in a system where a CPU 311, a ROM/RAM 312, an input unit 313, an output unit 314, an

BNSDOCID: <GB__2331381A_I_>
BNSDOCID: <GB 2331381A I>

external storage unit 315, a medium driving unit 316, a portable storage medium 319 and a network connecting unit 317 are connected via a bus. That is, it is needless to say that the functions of the present invention can also be implemented by providing a system or apparatus with a ROM/RAM 312, an external storage unit 315 and a portable storage medium 319, in which software program codes for implementing the system of each above-mentioned embodiments are recorded, and executing the reading of the program codes by the computer (or CPU 311) of the system or apparatus.

In this case, the read program codes themselves implement the new functions of the present invention, and the portable storage medium 319, etc. in which the program codes are recorded only constructs the present invention.

As a portable storage medium 319 for supplying program codes, for example, a floppy disk, a hard disk, a magneto-optic disk, an optical disk, a CD-ROM, a CD-R, a magnetic tape, a nonvolatile memory card, a ROM card, and various kinds of storage media storing the program codes accessed via a network connecting unit 317 (in other words, a communication circuit) such as an electronic mail, personal computer

BNSDOCID <GB 2331381A 1 >
BNSDOCID: <GB 2331381A 1 >

communication, etc. can be used.

By executing the program codes read by a computer, an OS operating in the computer, etc. executes a part or all of the actual process according to the instruction of the program codes, and thereby the functions of the above-mentioned embodiments can be implemented.

Furthermore, after the read program codes are written in a memory provided in a feature expansion board inserted in a computer or a feature expansion unit connected to a computer, a CPU provided in the feature expansion board or unit, etc. executes a part or all of the actual process, and thereby the functions of the above-mentioned embodiments can also be implemented.

As described so far, in the present invention a secure area is usually prevented from being accessed by users by means of, for example, the firmware of a storage unit, and as a result, authenticators, access logs, etc. related to data files cannot be altered.

By locating files and access logs, etc. related to data files in a non-secure area being a normal area and locating only the authenticators of the files in a secure area, the size of the secure area can be reduced.

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB_ 2331381A_I_>

CLAIMS:

1. A system for managing files comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storage unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing the access allowing keys; and

file accessing means (13) for sending an access request together with the access allowing key, and

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are authenticated with each other, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys;

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access

BNSDOCID: <GB 2331381A I >

allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area usually unaccessible.

2. The system for managing files according to claim 1, wherein the reciprocal authenticating means (11) provided in said computer (1) and said file accessing means (13) are implemented by a unit of hardware.

3. A system for managing files, comprising:

sub-file storing means (138) for storing one or a plurality of sub-files (34) related to a main-file (33);

authentication information creating means (14) for creating sub-file authentication information used to verify the sub-files (34); and

system file storing means (134) for storing a system file (35) to which the sub-file authentication information is related.

4. A system for managing files, comprising:

main-file storing means (136) for storing a main-file (33);

BNSDOCID: <GB___2371381A_I_>
BNSDOCID: <GB__ : 1A I >

authentication information creating means (14) for creating main-file authentication information to be used to verify the main-file (33); and

sub-file storing means (138) for storing at least one sub-file (34) to which the main-file authentication information is related.

5. A system for managing files, comprising:

main-file storing means (136) for storing a main-file (33);

sub-file storing means (138) for storing at least one sub-file (34) to which the main-file authentication information is related;

authentication information creating means (14) for creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files (34); and

system file storing means (134) for storing a system file (35) to which the sub-file authentication information is related.

6. The system for managing files according to claim 5, wherein said main-file (33), said sub-files (34) and said system files (35) are stored in a non-secure

BNSDOCID <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

area (32) usually accessible.

7. The system for managing files according to claim 5, wherein said main-file (33), and said sub-files (34) and said system files (35) are stored in a non-secure area (32) usually accessible and a secure area (31) usually unaccessible, respectively.

8. The system for managing files according to claim 5, wherein said main-file (33) and said sub-files (34), and said system files (35) are stored in a non-secure area (32) usually accessible and a secure area (31) usually unaccessible, respectively.

9. The system for managing files according to claim 6, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storage unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing the access allowing keys; and

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB_ _ 2331381A_ _I_>

file accessing means (13) for sending an access request together with the access allowing key,

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area 3 1), and uses the medium ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

BNSDOCID: <GB 2331381A_1 >
BNSDOCID: <GB 2331381A_1 >

10. The system for managing files according to claim 7, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storage unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing all the access allowing keys; and

file accessing means (13) for sending an access request together with the access allowing key,

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access allowing key storing means (12) and at least one

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB_ _2331381A I >

access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area (31), and uses the medium ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

11. The system for managing files according to claim 8, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storing unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing the access allowing key; and

file accessing means (13) for sending an access request together with the access allowing key.

BNSDOCID: <GB 2331381A I >
BNSDOCID: <GB 2331381A I >

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area (31), and uses the medium ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

12. The system for managing files according to claim

BNSDOCID: <GB_ 2331381A_I_>
BNSDOCID: <GB_ 2331381A_I_>

9, wherein

the reciprocal authenticating means (11) provided in said computer (1) and said file accessing means (13) are implemented by means of hardware.

13. The system for managing files according to claim 9, wherein

the medium ID (36) is a card ID (18).

14. The system for managing files according to claim 9, wherein

the medium ID (36) is a master ID (17).

15. The system for managing files according to claim 9, wherein

said authentication information is created for each record of a file.

16. The system for managing files according to claim 10, wherein

said authentication information is created for each record of a file.

17. The system for managing files according to claim 11, wherein

BNSDOCID: <GB 2331381A I >
BNSDOCID: <GB 2331381A I >

said authentication information is created for each record of a file.

18. A system for managing files, comprising:

sub-file reading means (139) for reading one or a plurality of sub-files (34) related to a main-file (33);

authentication information creating means (14) for creating sub-file authentication information from sub-files (34) read by the sub-file reading means (139);

system file reading means (135) for reading sub-file authentication information from a system file (35) related to the sub-file (34); and

authentication information comparing means (15) for comparing the sub-file authentication information created by the authentication information creating means (14) with the sub-file authentication information read by the system file reading means (135).

19. A system for managing files, comprising:

main-file reading means (137) for reading a main-file (33);

authentication information creating means (14)

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB_ _2331381A_I_>

for creating main-file authentication information from a main-file (33) read by the main-file reading means (137);

sub-file reading means (139) for reading main-file authentication information from sub-files (34) related to the main-file (33); and

authentication information comparing means (15) for comparing the main-file authentication information created by the authentication information creating means (14) with the main-file authentication information read by the sub-file reading means (139).

20. A system for managing files, comprising:

main-file reading means (137) for reading a main-file (33);

sub-file reading means (139) for reading main-file authentication information from sub-files (34) related to the main-file (33) and one or a plurality of sub-files (34) related to the main-file (33);

system file reading means (135) for reading sub-file authentication information from a system file (35) related to the sub-file (34);

authentication information creating means (14) for creating main-file authentication information from a main-file (33) read by the main-file reading means

BNSDOCID: <GB 2331381A 1 >

(137) and creating sub-file authentication information from sub-files (34) read by the sub-file reading means (139); and

an authentication information comparing means (15) for comparing the main-file authentication information created by the authentication information creating means (14) with the main-file authentication information read by the sub-file reading means (139) and comparing the sub-file authentication information created by the authentication information creating means (14) with the sub-file authentication information read by the system file reading means (135).

21. The system for managing files according to claim 20, wherein said main-file (33), said sub-files (34) and said system file (35) are stored in a non-secure area (32) usually accessible.

22. The system for managing files according to claim 20, wherein said main-file (33), and said sub-files (34) and said system file (35) are stored in a non-secure area (32) usually accessible and a secure area (31) usually unaccessible, respectively.

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB __2331381A I >

23. The system for managing files according to claim 20, wherein said main-file (33) and said sub-files (34), and said system file (35) are stored in a non-secure area (32) usually accessible and a secure area (31) usually unaccessible, respectively.

24. The system for managing files according to claim 21, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storing unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing the access allowing keys; and

file accessing means (13) for sending an access request together with the access allowing key.

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

BNSDOCID <GB 2331381A_I_>
BNSDOCID <GB 2331381A I >

access allowing key group storing means (22) for storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area (31), and uses the medium ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

25. The system for managing files according to claim 22, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storing unit (2) and when the computer (1) and the

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing the access allowing key; and

file accessing means (13) for sending an access request together with the access allowing key,

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means (13) and stored in the access allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area (31), and uses the medium

BNSDOCID <GB 2331381A 1 >
BNSDOCID <GB 2331381A 1 >

ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

26. The system for managing files according to claim 23, further comprising a computer (1) and a storage unit (2), wherein

the computer (1) comprises

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with the storing unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key storing means (12) for storing all the access allowing keys; and

file accessing means (13) for sending an access request together with the access allowing key,

the storage unit (2) comprises

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with the computer (1) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys;

access allowing key group storing means (22) for

BNSDOCID <GB __2331381A__I_>
BNSDOCID: <GB __2331381A_I_>

storing all the access allowing keys; and

access allowing key identification means (23) for identifying if the access allowing key sent from the file accessing means and stored in the access allowing key storing means (13) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible, and

the authentication information creating means (14) reads a medium ID (36) peculiar to the medium stored in the secure area (31), and uses the medium ID (36) to create the main-file authentication information and the sub-file authentication information after the computer (1) and the storage unit (2) are reciprocally authenticated.

27. The system for managing files according to claim 24, wherein

the reciprocal authenticating means (11) provided in said computer (1) and said file accessing means (13) are implemented by means of hardware.

28. The system for managing files according to claim 24, wherein

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

the medium ID (36) is a card ID (18).

29. The system for managing files according to claim 24, wherein

the medium ID (36) is a master ID (17).

30. The system for managing files according to claim 24, wherein

said authentication information is created for each record of a file.

31. The system for managing files according to claim 1, wherein

said secure area accessing means (24) further comprises

access control information reading means (241) for reading access control information (38) stored in said secure area (31), and

said storage unit (2) further comprises

sector accessing means (251) for accessing a main-file (33) or sub-files (34) related to the main-file (33) in units of sectors or sector groups according to the access control information (38).

32. The system for managing files according to claim

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB _ 2331381A _I_>

31, wherein

said secure area accessing means (24) further comprises

access control information setting means (242) for setting access control information (38) in said secure area (31).

33. The system for managing files according to claim 9, wherein

authentication information is created using one, two or all of said medium ID (36), said card ID (18) and said master ID (17).

34. The system for managing files according to claim 24, wherein

authentication information is created using one, two or all of said medium ID (36), said card ID (18) and said master ID (17).

35. A computer (1), comprising:

reciprocal authenticating means (11) for reciprocally authenticating the computer (1) with a storing unit (2) and when the computer (1) and the storage unit (2) are reciprocally authenticated, creating access allowing keys; and

BNSDOCID: <GB 2331381A 1>

access allowing key storing means (12) for storing the access allowing keys; and

file accessing means (13) for sending an access request together with the access allowing key.

36. A storage unit (2), comprising:

reciprocal authenticating means (21) for reciprocally authenticating the storage unit (2) with a computer (1) and when the computer (1) and the storage unit (2) are authenticated with each other, creating access allowing keys;

access allowing key group storing means (22) for storing all the access allowing keys;

access allowing key identification means (23) for identifying if the access allowing key stored in the access allowing key storing means (12) and at least one access allowing key stored in the access allowing key group storing means (22), are the same; and

secure area accessing means (24) for accessing a secure area (31) usually unaccessible.

37. A method of managing files, comprising the steps of:

reciprocally authenticating between a computer and a storage unit and when the computer and the

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

storage unit are reciprocally authenticated, creating an access allowing key;

storing the access allowing key;

storing all the access allowing keys;

sending an access request together with the access allowing key;

identifying if the access allowing key stored in the access allowing key storing step and at least one access allowing key stored in the access allowing key group storing step, are the same; and

accessing a secure area usually unaccessible.

38. A method of managing files, comprising the steps of:

storing one or a plurality of sub-files related to a main-file;

creating sub-file authentication information used to verify the sub-files; and

storing a system file to which the sub-file authentication information is related.

39. A method of managing files, comprising the steps of:

storing a main-file;

creating main-file authentication information to

BNSDOCID <GB 2331381A I>
BNSDOCID: <GB 2331381A I>

be used to verify the main-file; and

storing at least one sub-file to which the main-file authentication information is related.

40. A method of managing files, comprising the steps of:

storing a main-file;

storing at least one sub-file to which the main-file authentication information is related;

creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

storing a system file to which the sub-file authentication information is related.

41. A method of managing files, comprising the steps of:

reading one or a plurality of sub-files related to a main-file;

creating sub-file authentication information from sub-files;

reading sub-file authentication information from a system file related to the sub-file; and

comparing the sub-file authentication information

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB_ _2331381A I >>

from the sub-files with the sub-file authentication information from the system file.

42. A method of managing files, comprising the steps of:

reading a main-file;

creating main-file authentication information from the main-file;

reading main-file authentication information from sub-files related to the main-file; and

comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

43. A method of managing files, comprising the steps of:

reading a main-file;

reading main-file authentication information from sub-files related to the main-file and one or a plurality of sub-files related to the main-file;

reading sub-file authentication information from a system file related to the sub-file;

creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

BNSDOCID <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I>

comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the system file with the sub-file authentication information from the sub-file.

44. A method of managing files, comprising the steps of:

reciprocally authenticating a computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

storing the access allowing keys; and

sending an access request together with the access allowing key.

45. A method of managing files, comprising the steps of:

reciprocally authenticating a storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

storing all the access allowing keys;

identifying if the access allowing key and at

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

least one access allowing key, are the same; and

accessing a secure area usually unaccessible.

46. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

a reciprocal authenticating step of reciprocally authenticating between a computer and a storage unit and when the computer and the storage unit are reciprocally authenticated, creating an access allowing key;

an access allowing key storing step of storing the access allowing key;

an access allowing key group storing step of storing all the access allowing keys;

a file accessing step of sending an access request together with the access allowing key;

an access allowing key identifying step of identifying if the access allowing key stored in the access allowing key storing process and at least one access allowing key stored in the access allowing key group storing step, are the same; and

a secure area accessing step of accessing a secure area usually unaccessible.

BNSDOCID <GB 2331381A_I_>

47. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file storing step of storing one or a plurality of sub-files related to a main-file;

authentication information creating step of creating sub-file authentication information used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

48. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file storing step of storing a main-file;

authentication information creating step of creating main-file authentication information to be used to verify the main-file; and

sub-file storing step of storing at least one sub-file to which the main-file authentication information is related.

49. A computer readable storage medium having a recorded file management program for enabling a

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

computer to execute:

main-file storing step of storing a main-file;

sub-file storing step of storing at least one sub-file to which the main-file authentication information is related;

authentication information creating step of creating main-file authentication information to be used to verify the main-file/sub-file authentication information to be used to verify the sub-files; and

system file storing step of storing a system file to which the sub-file authentication information is related.

50. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

sub-file reading step of reading one or a plurality of sub-files related to a main-file;

authentication information creating step of creating sub-file authentication information from sub-files;

system file reading step of reading sub-file authentication information from a system file related to the sub-file; and

authentication information comparing step of

BNSDOCID: <GB 2331381A I >

comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the system file.

51. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

authentication information creating step of creating main-file authentication information from a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to the main-file; and

authentication information comparing step of comparing the main-file authentication information from the main-file with the main-file authentication information from the sub-file.

52. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

main-file reading step of reading a main-file;

sub-file reading step of reading main-file authentication information from sub-files related to

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB__2331381A__I_>

the main-file and one or a plurality of sub-files related to the main-file;

system file reading step of reading sub-file authentication information from a system file related to the sub-file;

authentication information creating step of creating main-file authentication information from a main-file and creating sub-file authentication information from sub-files; and

authentication information comparing step of comparing the main-file authentication information from the sub-file with the main-file authentication information from the main-file and comparing the sub-file authentication information from the sub-file with the sub-file authentication information from the main-file.

53. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

reciprocal authenticating step of reciprocally authenticating a computer with a storing unit and when the computer and the storage unit are reciprocally authenticated, creating access allowing keys; and

access allowing key storing step of storing the

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I_>

access allowing keys; and

file accessing step of sending an access request together with the access allowing key.

54. A computer readable storage medium having a recorded file management program for enabling a computer to execute:

reciprocal authenticating step of reciprocally authenticating a storage unit with a computer and when the computer and the storage unit are authenticated with each other, creating access allowing keys;

access allowing key group storing step of storing all the access allowing keys;

access allowing key identification step of identifying if the access allowing key and at least one access allowing key, are the same; and

secure area accessing step of accessing a secure area usually unaccessible.

55. A system for managing files substantially as herein described with reference to and as shown in Figures 1 to 6, 7 and 8, 9, 10 and 11, 12 and 13, 14, 15, 16 and 17, 18 and 19, 20 and 21, 22 and 23, 24, 25, 26 and 27, 28 and 29, 30, or 31 of the accompanying drawings.

56. A method of managing files substantially as herein described with reference to Figures 1 to 6, 7 and 8, 9, 10 and 11, 12 and 13, 14, 15, 16 and 17, 18 and 19, 20 and 21, 22 and 23, 24, 25, 26 and 27, 28 and 29, 30, or 31 of the accompanying drawings.

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB__ 2331381A_I_>

The Patent Office

84

Application No: GB 9811875.5 **Examiner:** Geoffrey Western
Claims searched: 1,2,35-37,44,45,55,56 **Date of search:** 12 November 1998

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.P): G4A (AAP)

Int Cl (Ed.6): G06F 1/00 12/14

Other: Online: COMPUTER, EPODOC, WPI

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A	GB 1588147 A	(IBM)	-
X	WO 96/25700 A1	(ETA TECHNOLOGIES) N.b. abstract, Figs 7a,7d, pages 38-42	35,44, at least
A	WO 95/16947 A1	(HUGHES AIRCRAFT)	-
X	US 5610980 A	(JOHNSON et al) N.b. abstract, Figs 7a,7d, cols 34-38	35,44, at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB 2331381A_I_>

The Patent Office

Application No:	GB 9811875.5	**Examiner:**	K. Sylvan
Claims searched:	3,18,20,38,41,43,47,50,52,55,56 and claims dependent thereon.	**Date of search:**	15 February 1999

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP)

Int Cl (Ed.6): G06F (1/00)

Other: Online: Patents Citation Index

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	EP0281225 A2 HP. See abstract.	3,18,20,38,41,43,47,50,52 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

The Patent Office

86

Application No:	GB 9811875.5	**Examiner:**	K. Sylvan
Claims searched:	4,5,19,20,39,40,42,43,48, 49,51,52,55 and 56, and claims dependent thereon.	**Date f search:**	15 February 1999

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP)

Int Cl (Ed.6): G06F (1/00)

Other: Online: Patents Citation Index

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP0281225 A2	HP. See abstract.	4,5,19,20, 39,40,42, 43,48,49, 51,52 at least
X	US5619571	Sandstrom et al. See abstract.	4,19,39,42 ,48,51 at least
X	US5555303	Stambler. See abstract.	4,19,39,42 ,48,51 at least
X	US5479509	Ugon. See abstract.	4,19,39,42 ,48,51 at least
X	US5050212	Apple. See abstract.	4,19,39,42 ,48,51 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >

The Patent Office

87

Application No:	GB 9811875.5	**Examiner:**	K. Sylvan
Claims searched:	18,20,41-43,50-52 and claims dependent thereon.	**Date of search:**	15 February 1999

Patents Act 1977
Further Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.Q): G4A (AAP)

Int Cl (Ed.6): G06F (1/00)

Other: Online: Patents Citation Index

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP0281225 A2	HP. See page 1 lines 37-52.	18-20,41-43,50-52 at least
X	US5555303	Stambler. See column 2 lines 20-22.	19,42,51 at least
X	US5479509	Ugon. See column 3 lines 49-57..	19,42,51 at least
X	US5050212	Apple. See column 1 lines 54-61.	19,42,51 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB __ 2331381A _I_>

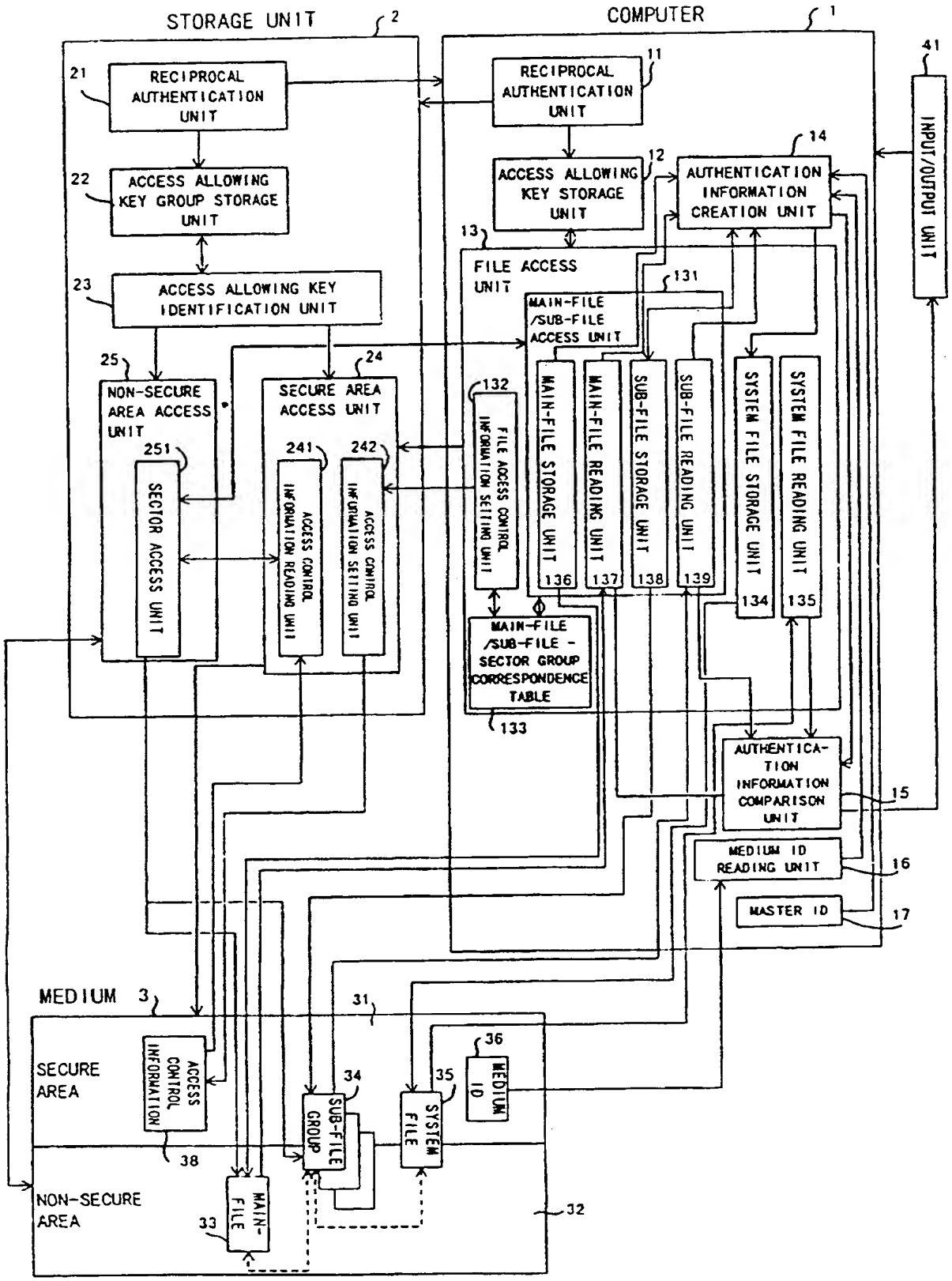

FIG. 1

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

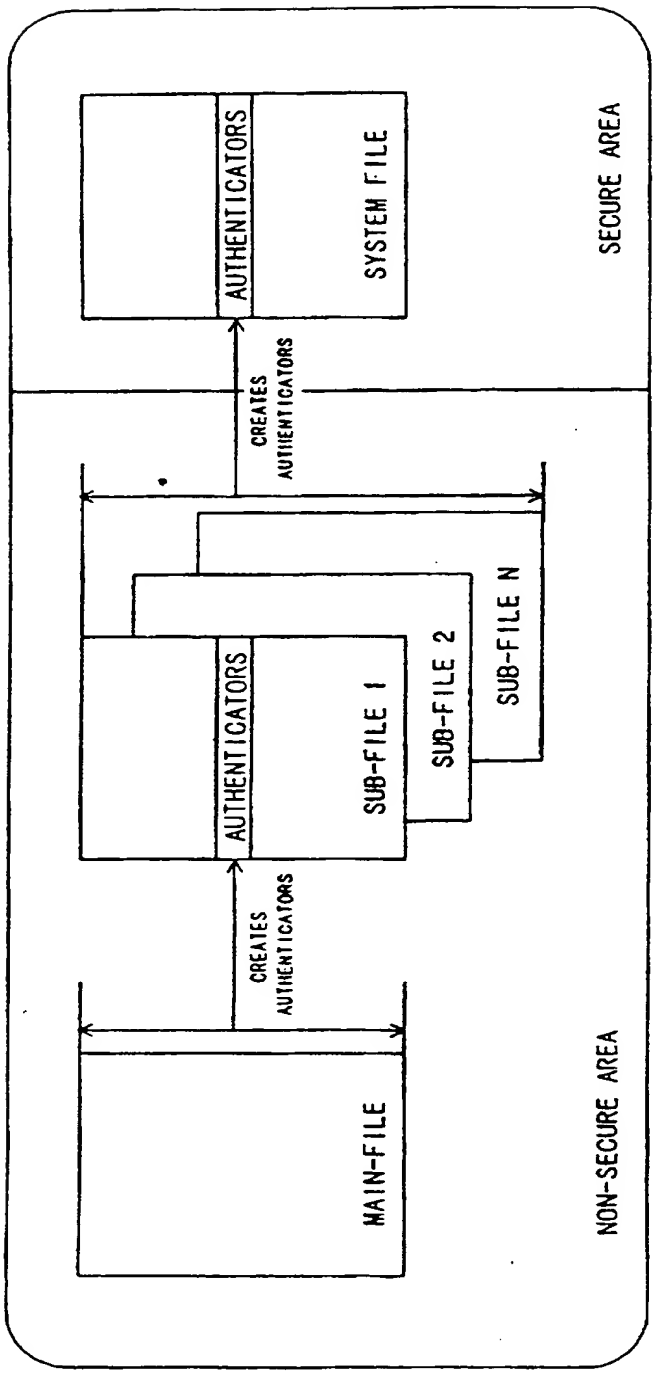

FIG. 2

BNSDOCID: <GB__ 2331381A__I_>
BNSDOCID: <GB__ 2331381A_ I_>

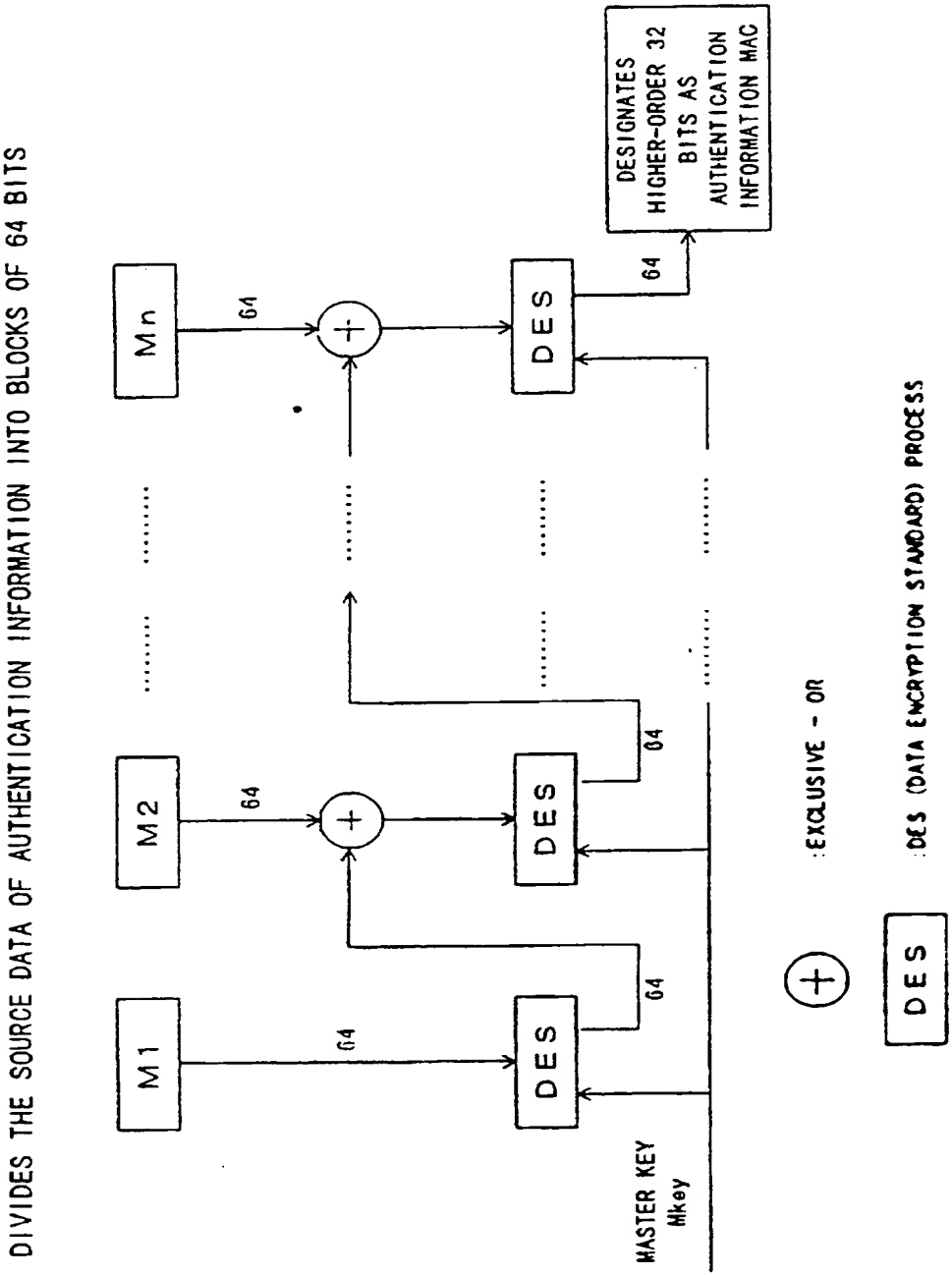

FIG. 3

BNSDOCID: <GB 2331381A I>
BNSDOCID: <GB 2331381A I>

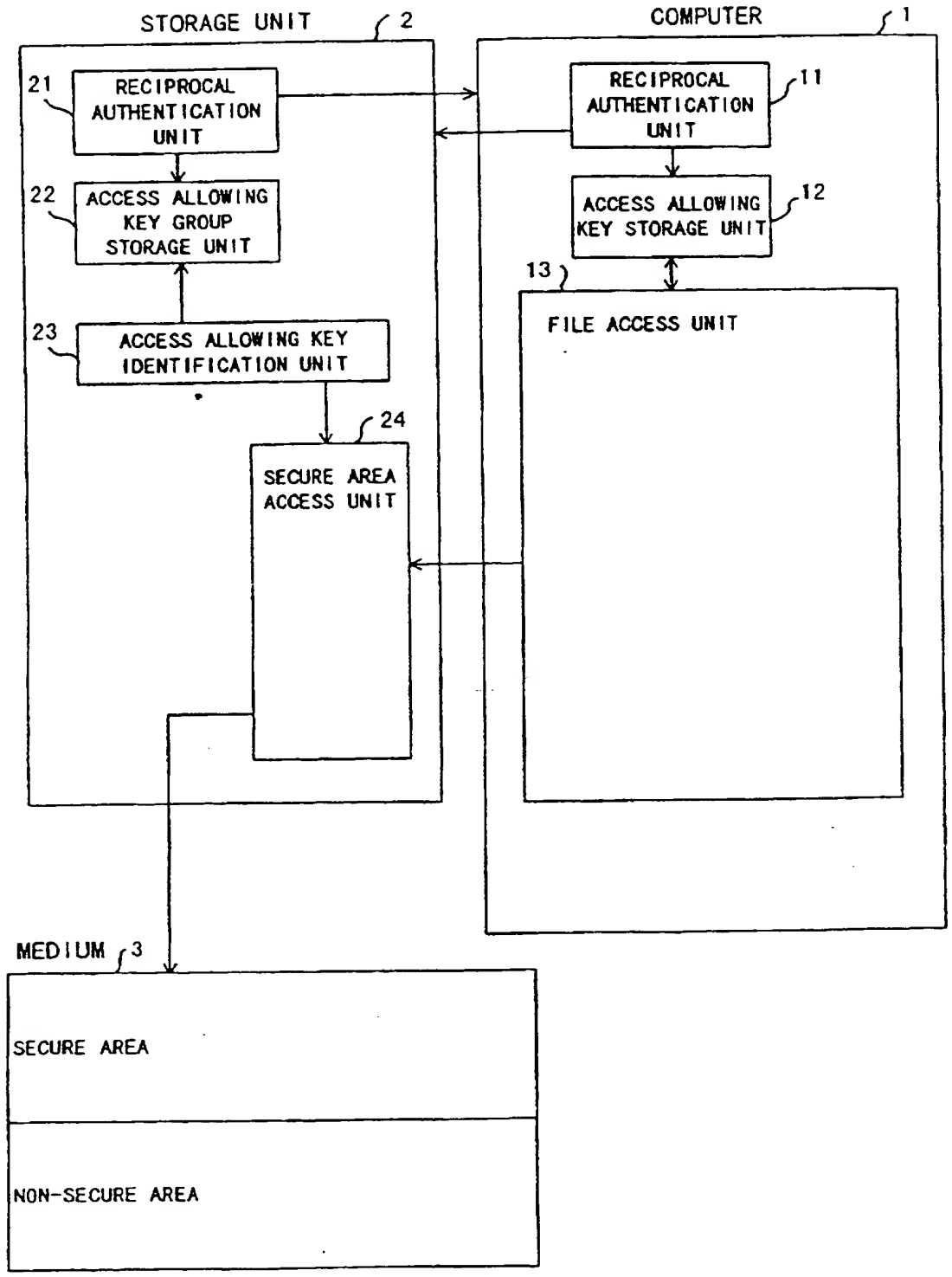

FIG. 4

BNSDOCID <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

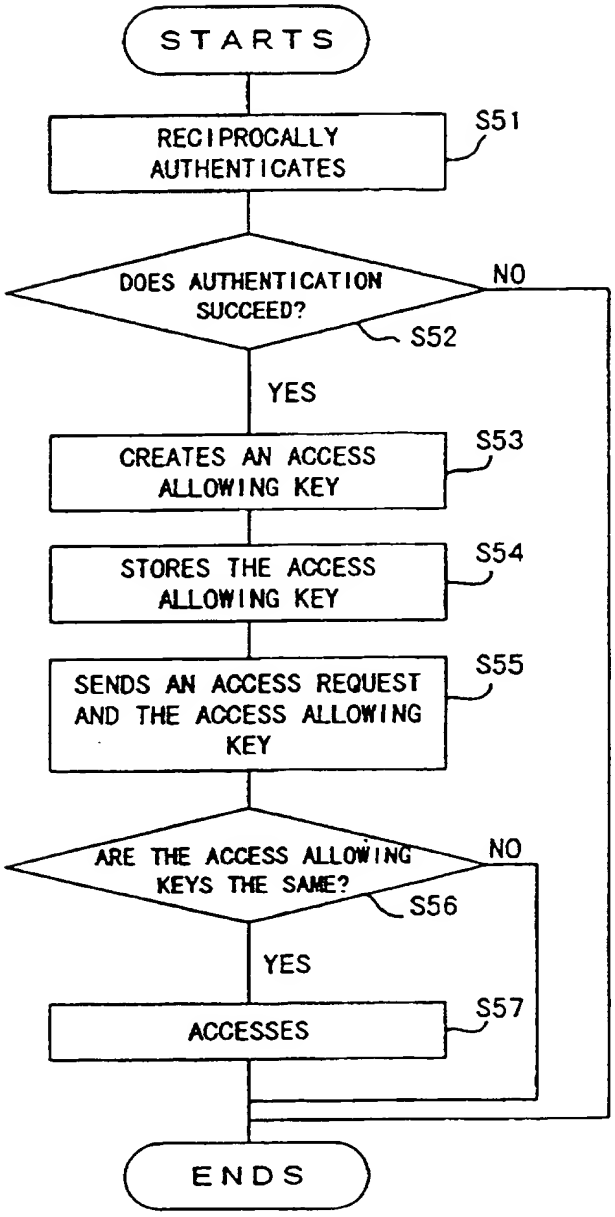

FIG. 5

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

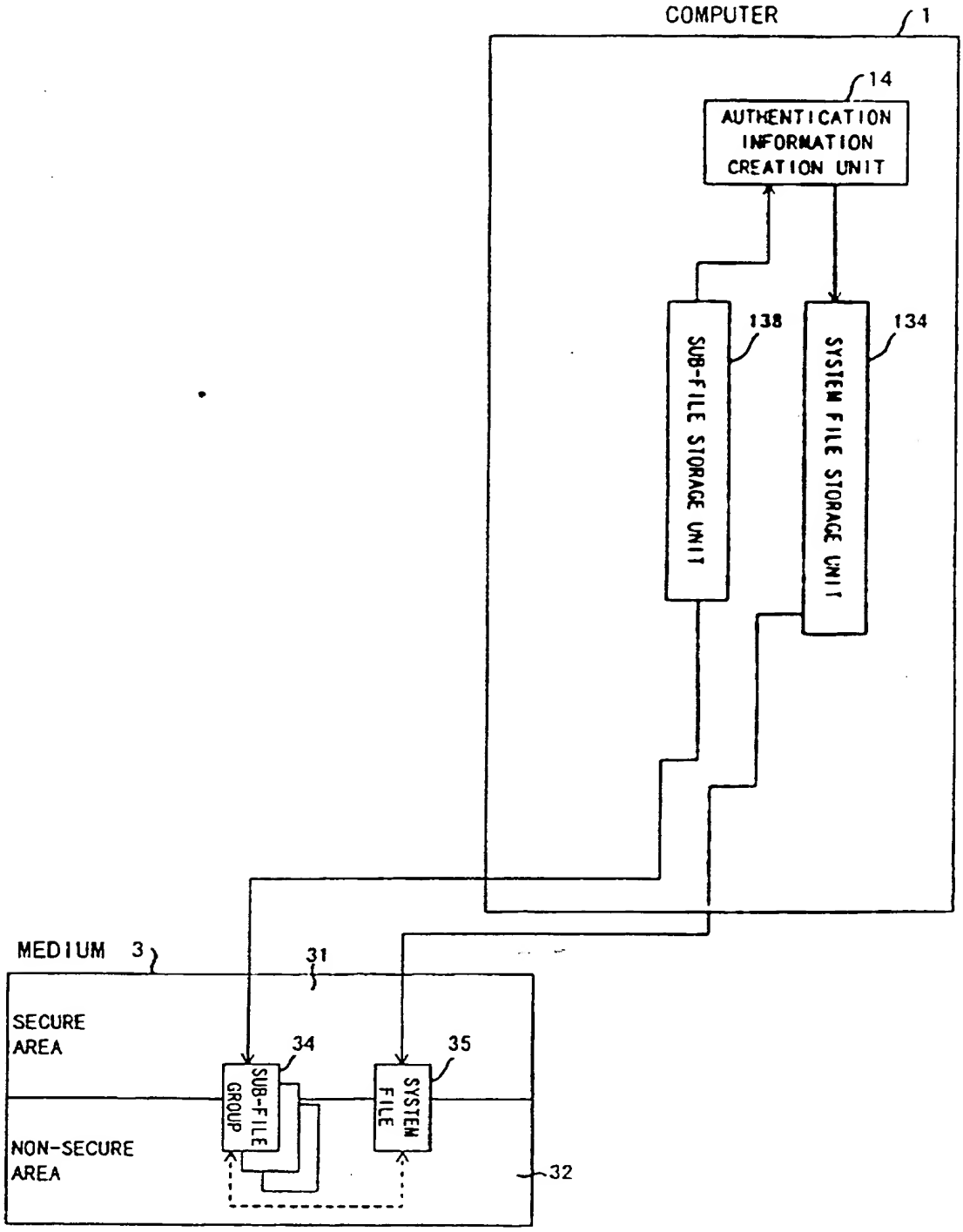

FIG. 6

BNSDOCID <GB__2331381A__I_>
BNSDOCID: <GB_ _2331381A _I_>

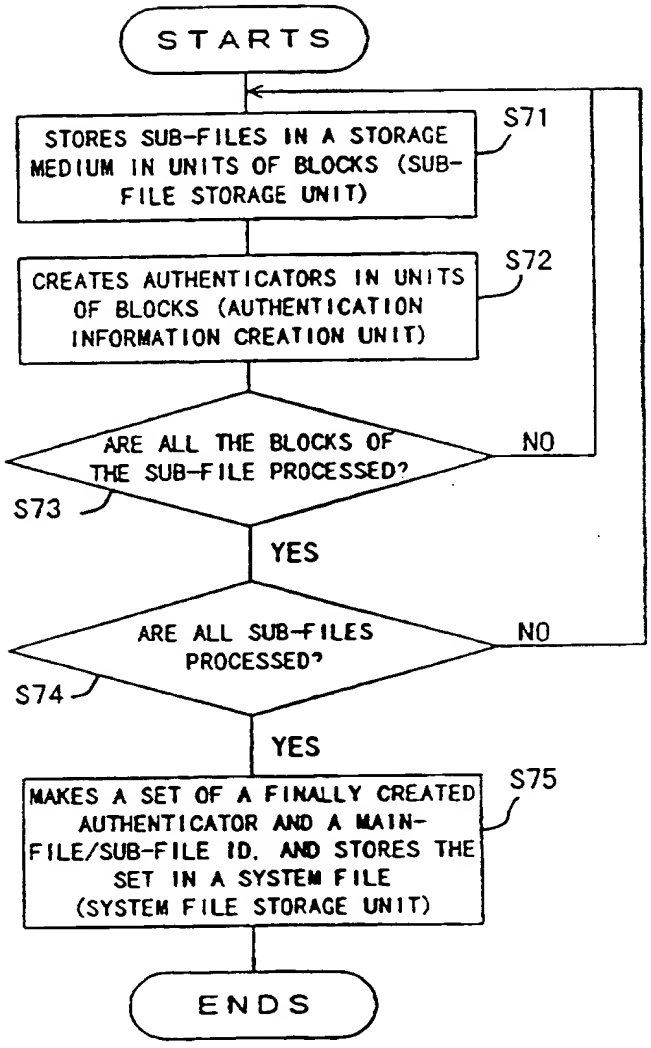

FIG. 7

BNSDOCID <GB___2331381A__I_>
BNSDOCID <GB___2331381A__I_>

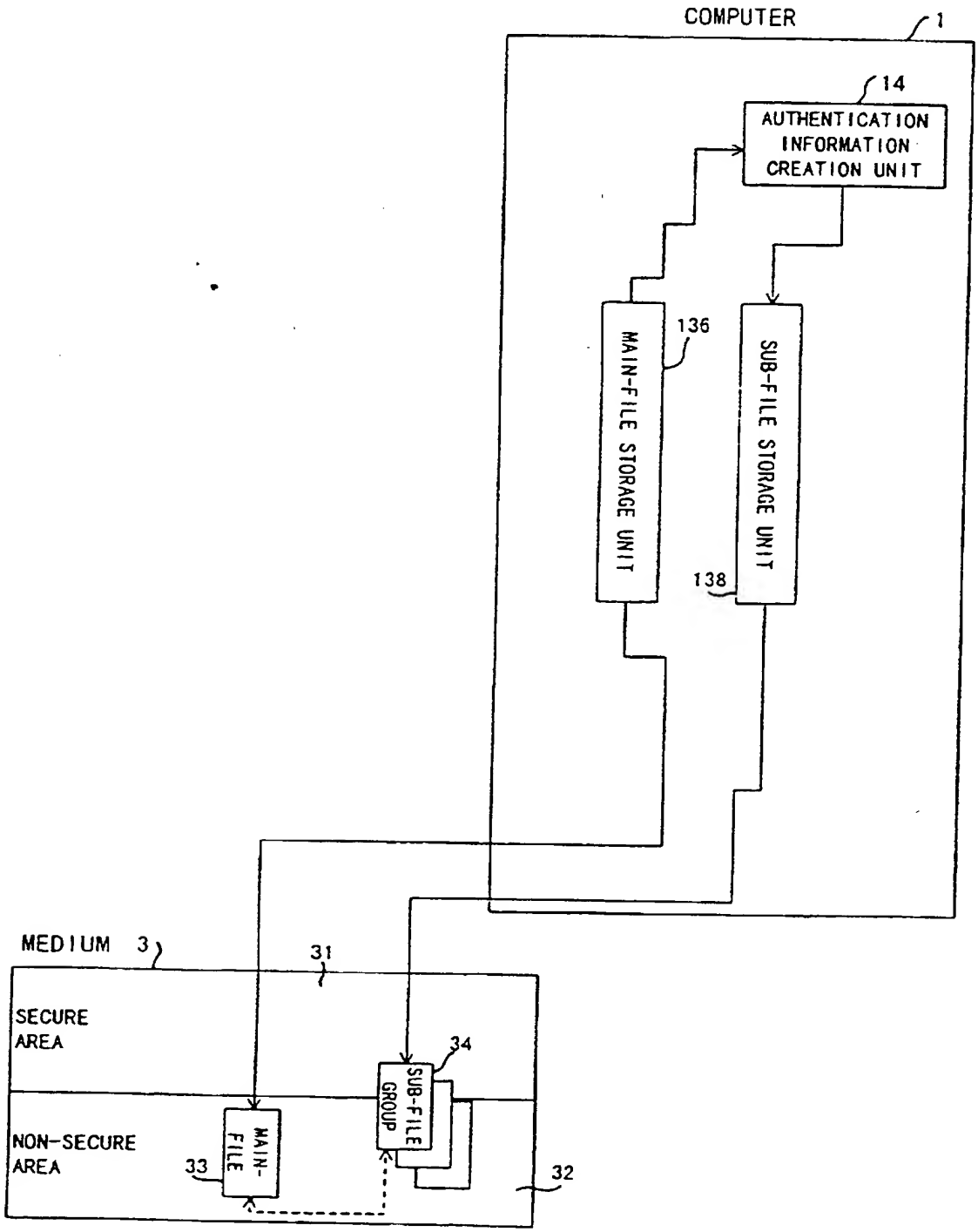

FIG. 8

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB__ 2331381A _I >>

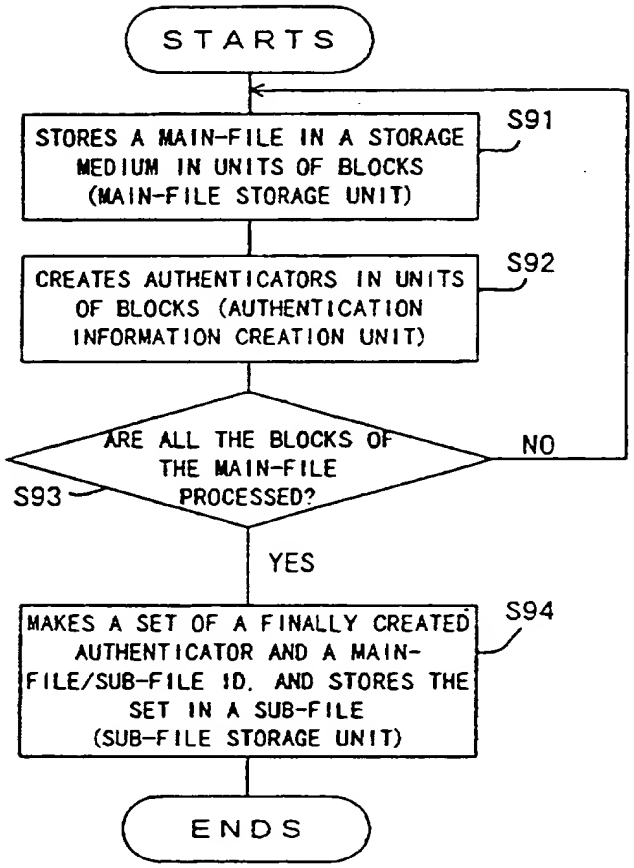

FIG. 9

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

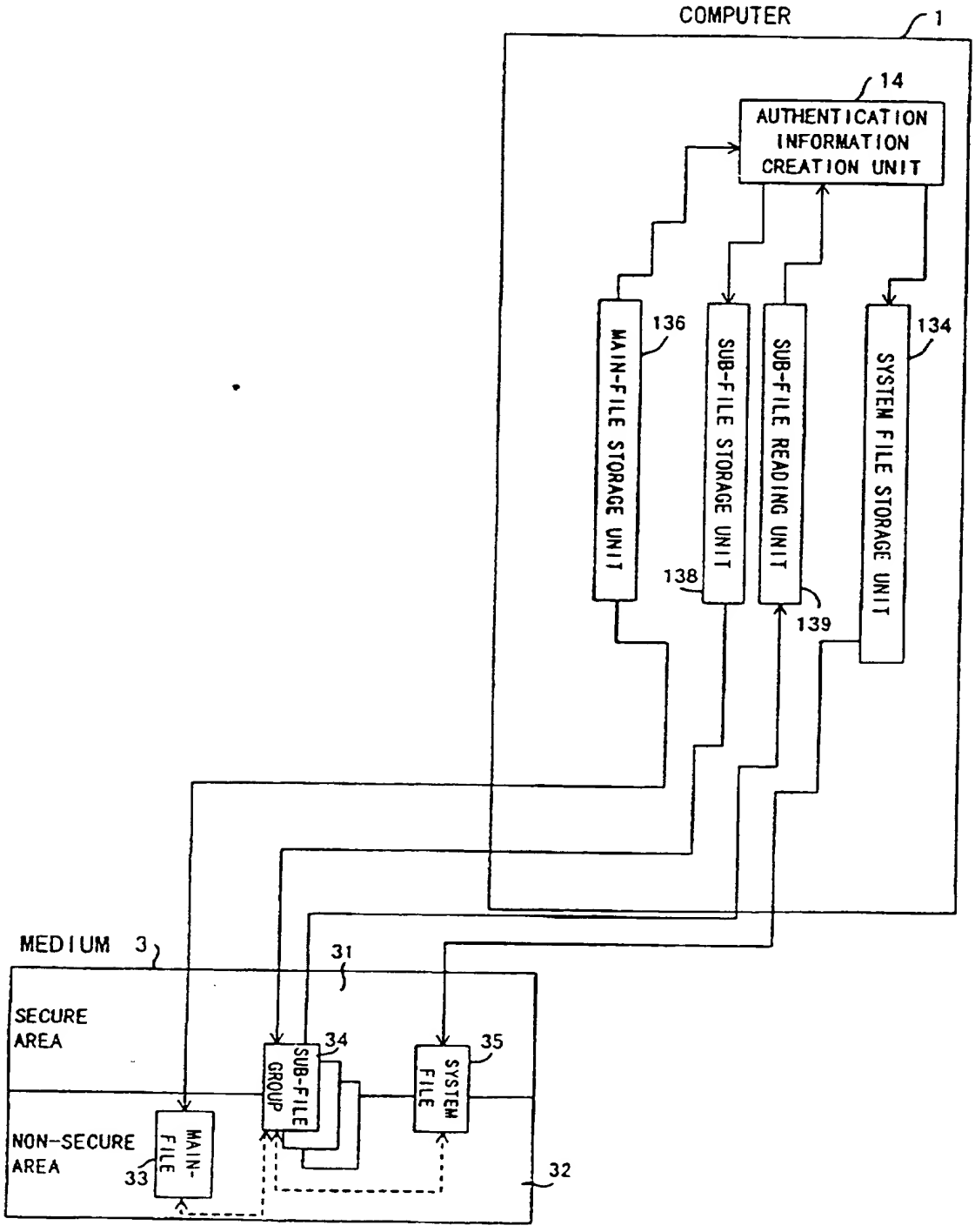

FIG. 10

BNSDOCID: <GB__2331381A__I_>
BNSDOCID: <GB__2331381A_I_>

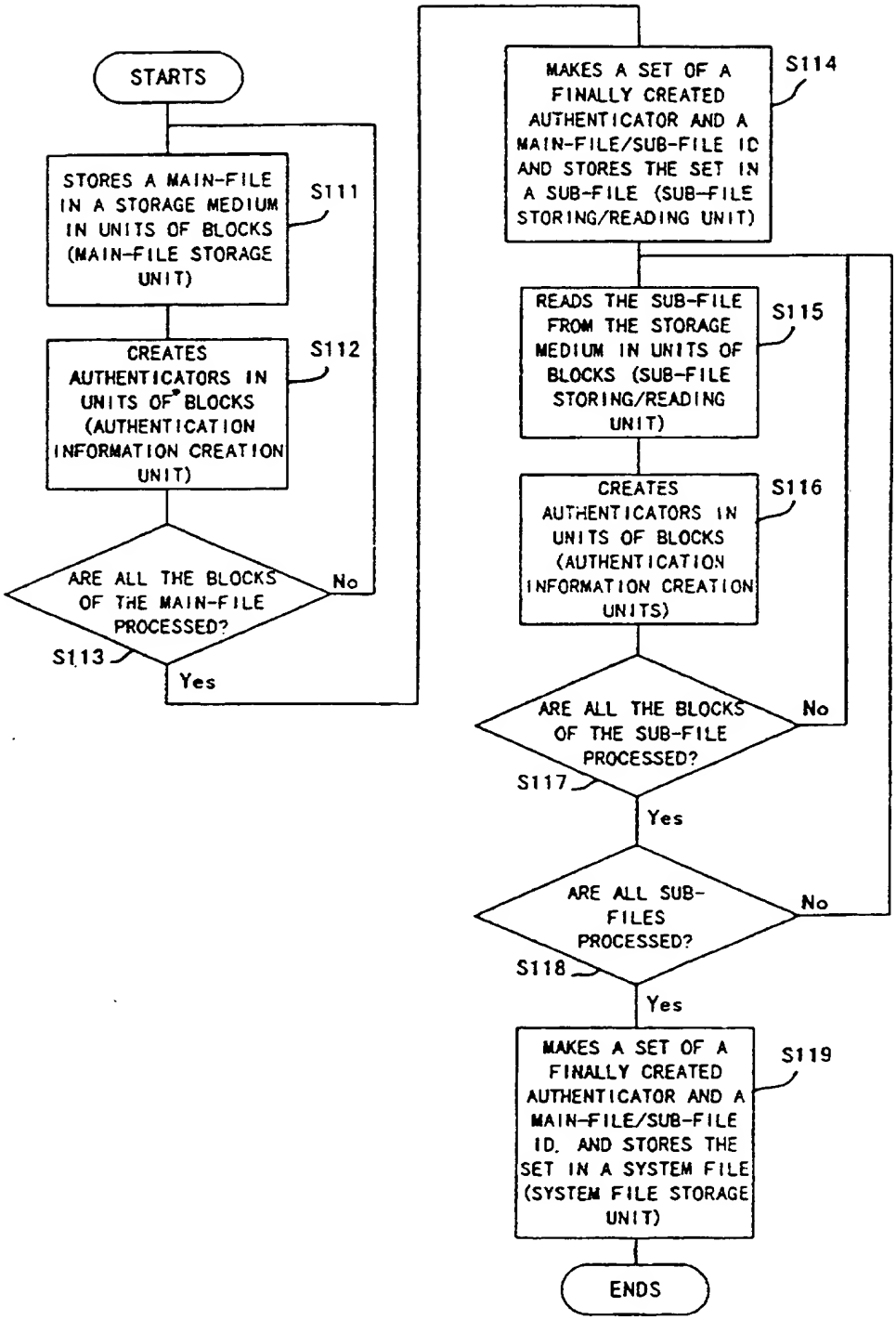

FIG. 11

BNSDOCID: <GB__2331381A__I_>
BNSDOCID: <GB 2331381A I>

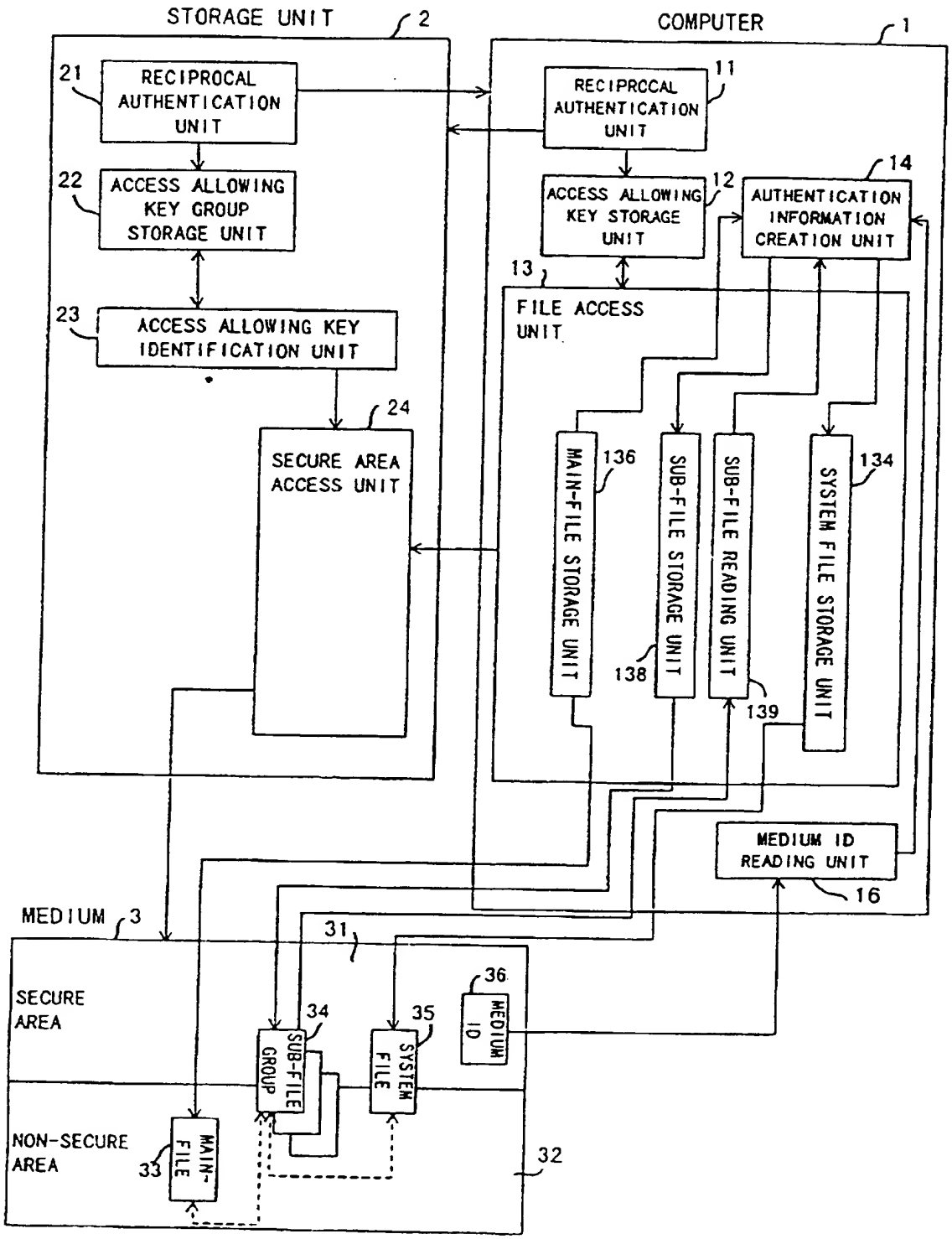

FIG. 12

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

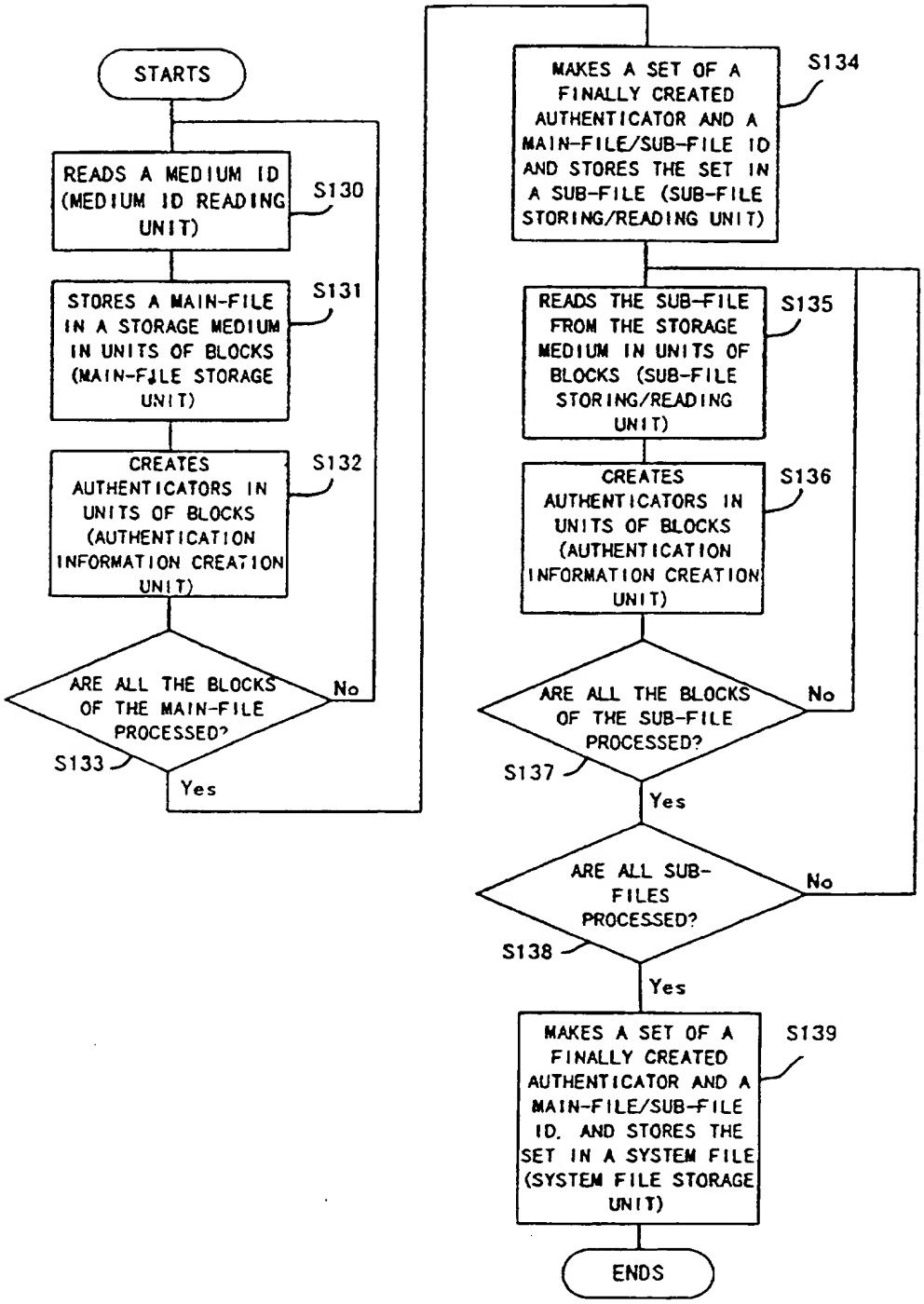

FIG. 13

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

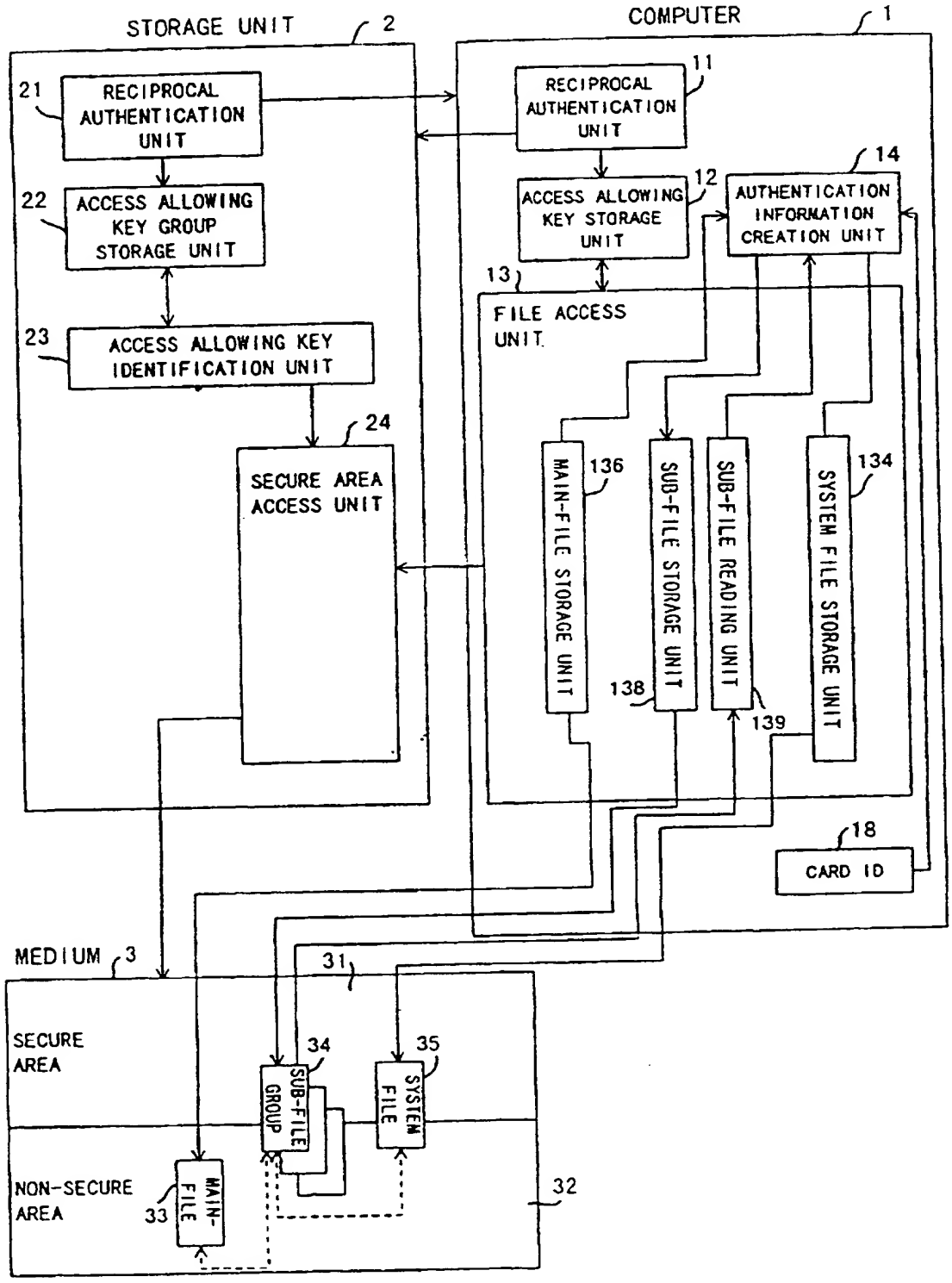

FIG. 14

BNSDOCID: <GB__2331381A_I_>
BNSDOCID: <GB__2331381A_I_>

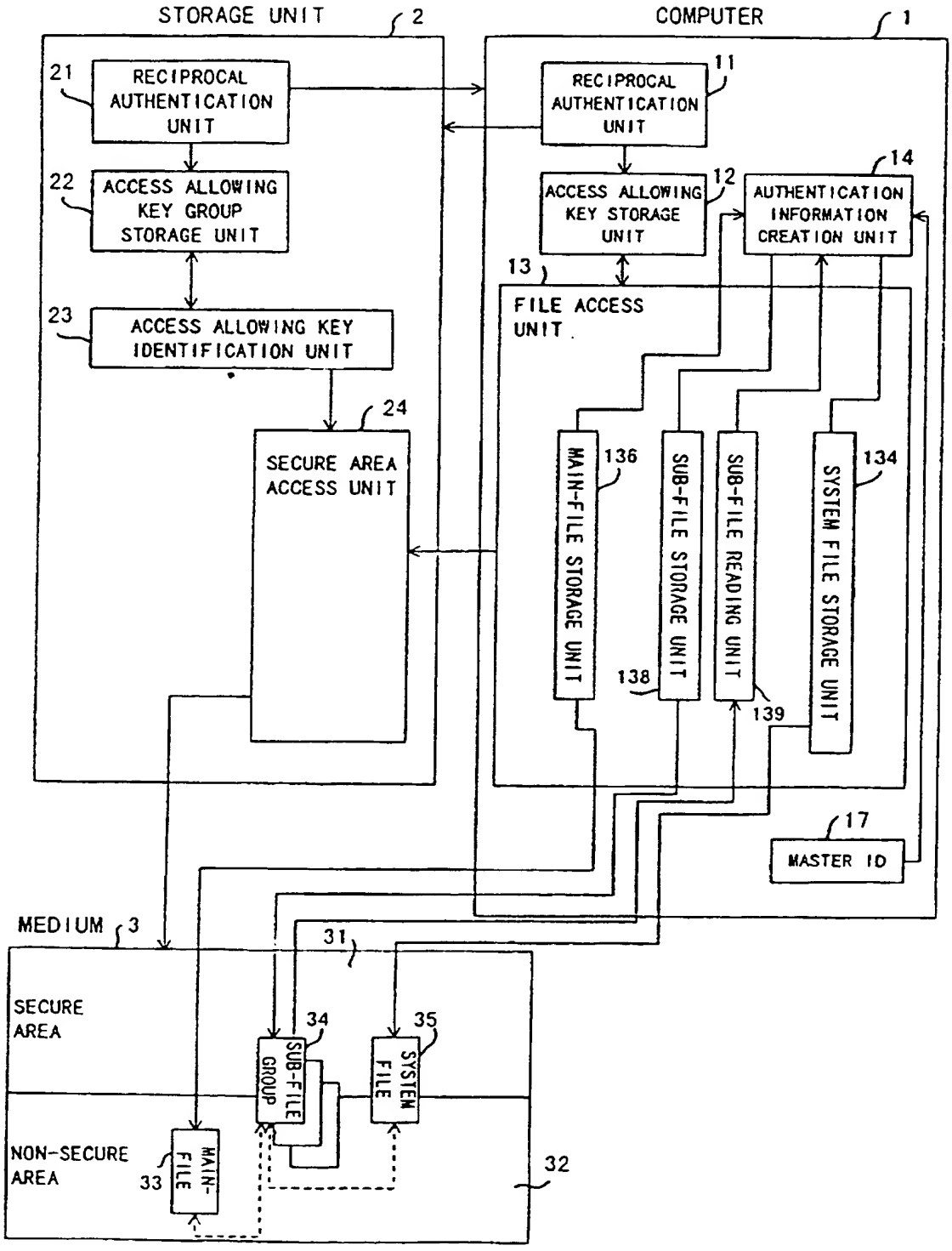

FIG. 15

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB 2331381A I >

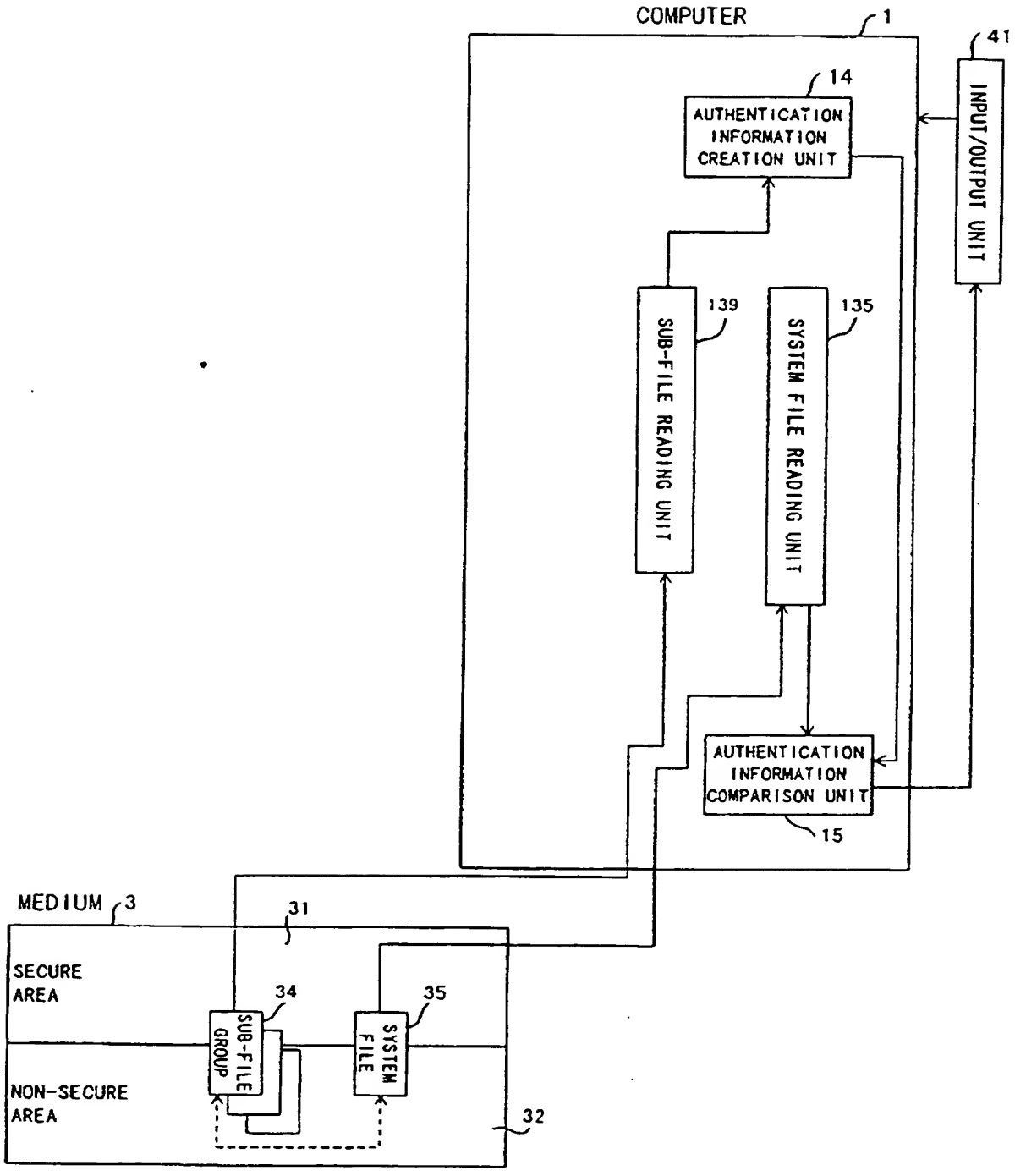

FIG. 16

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A_I_>

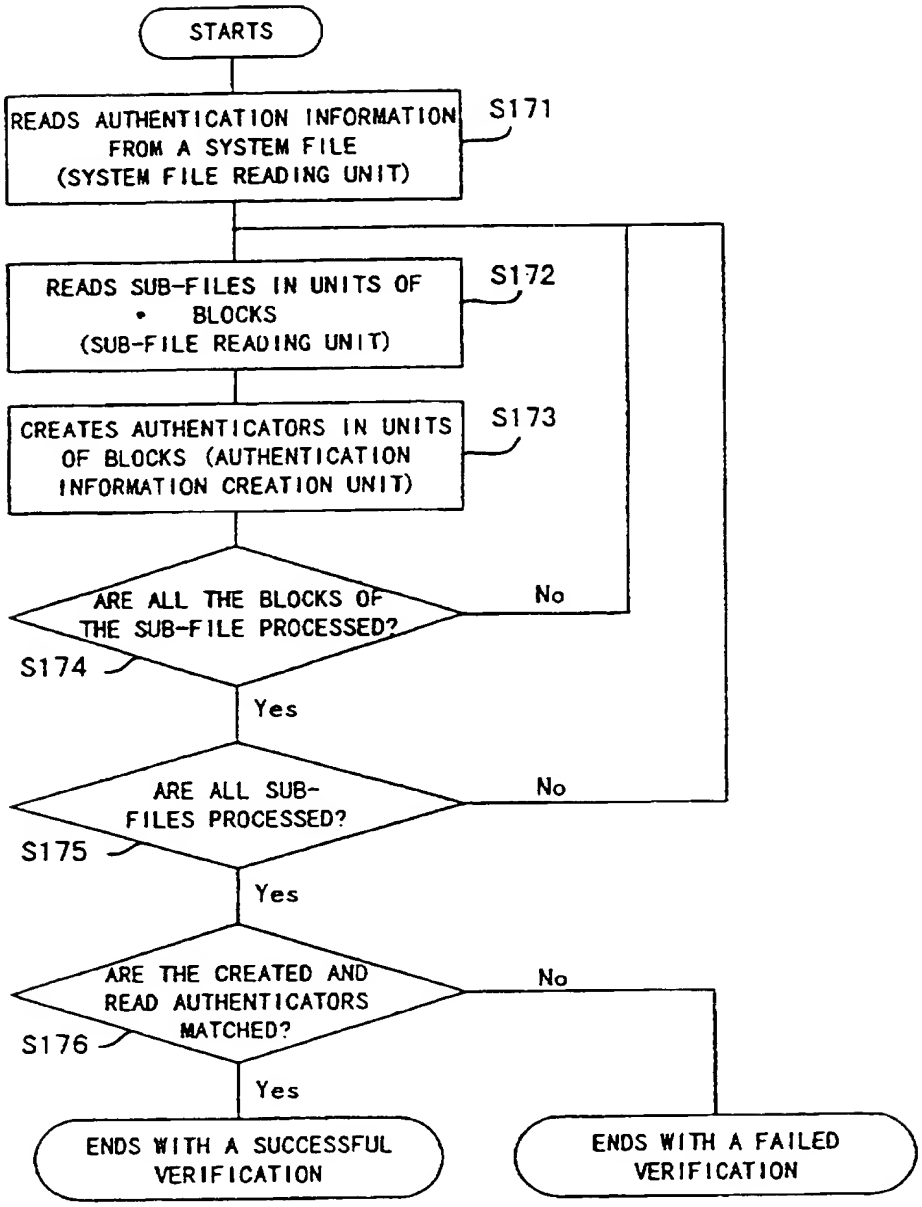

FIG. 17

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

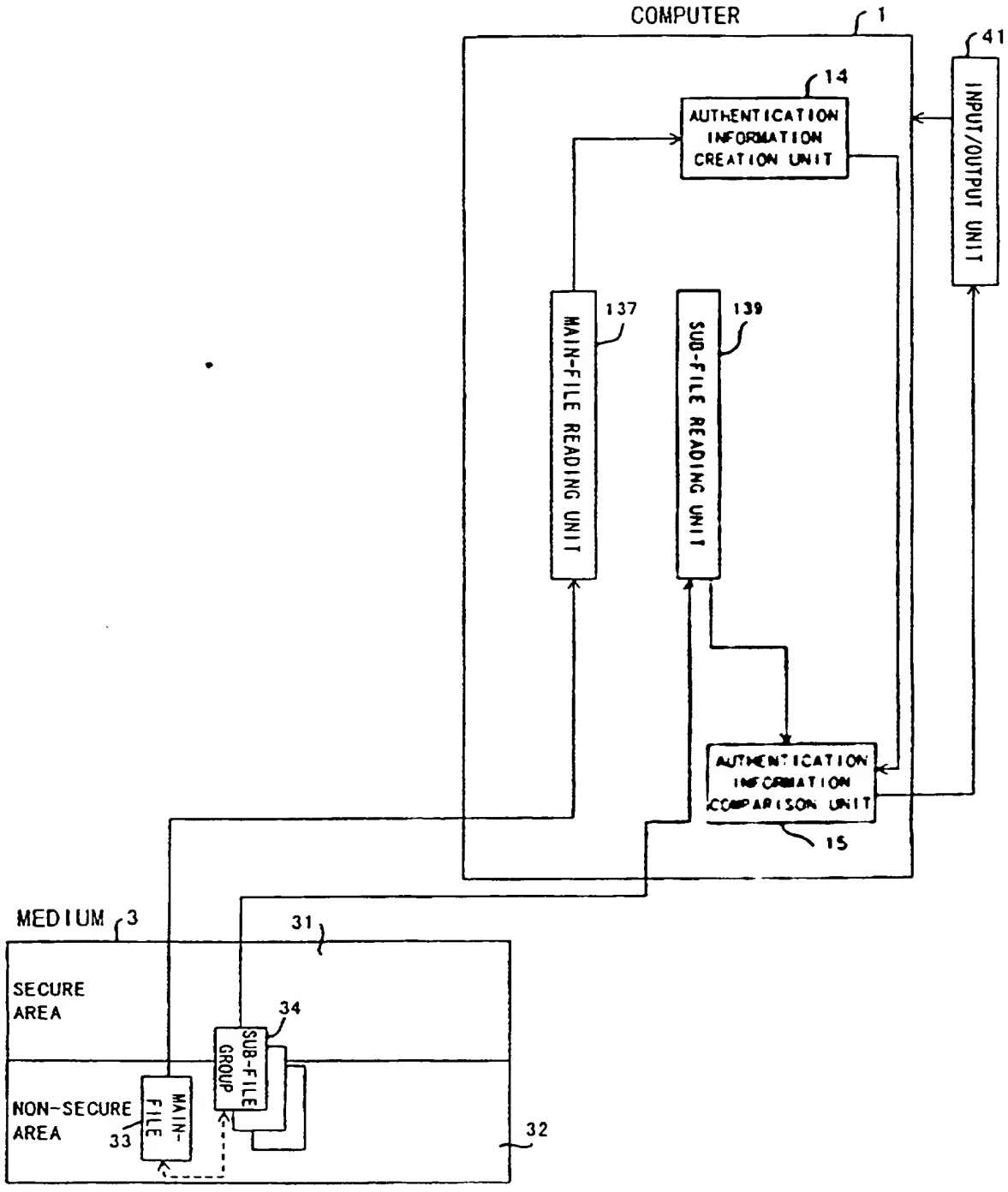

FIG. 18

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A_ I_>

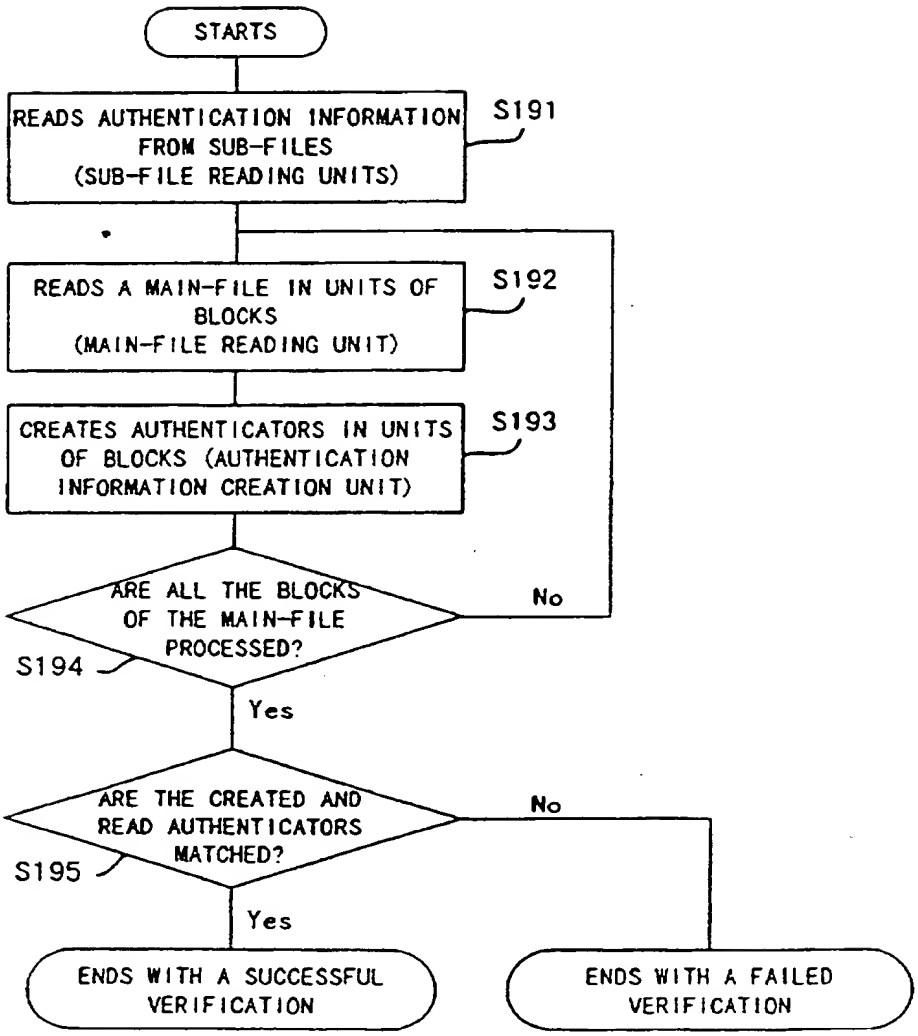

FIG. 19

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

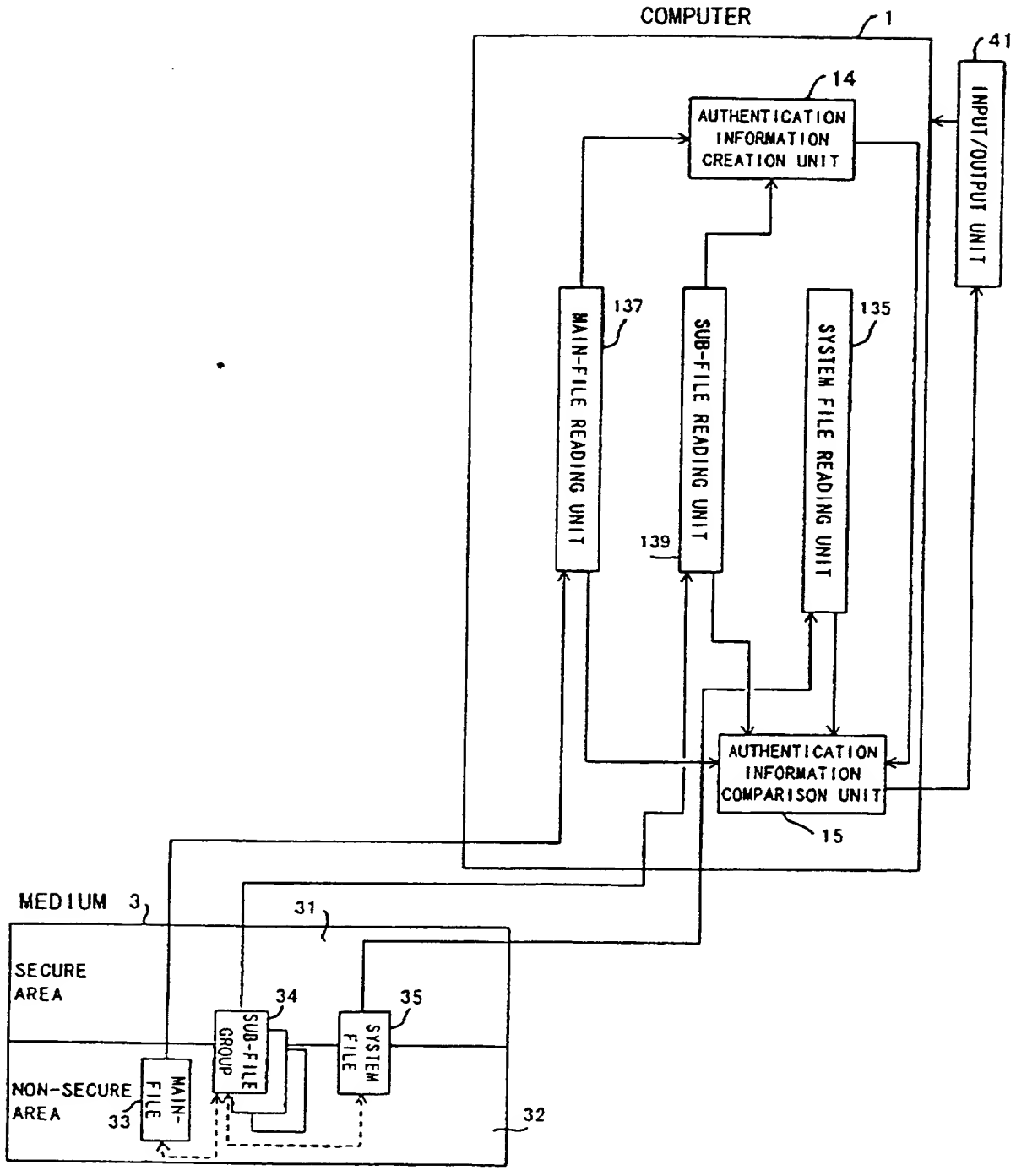

FIG. 20

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A_I_>

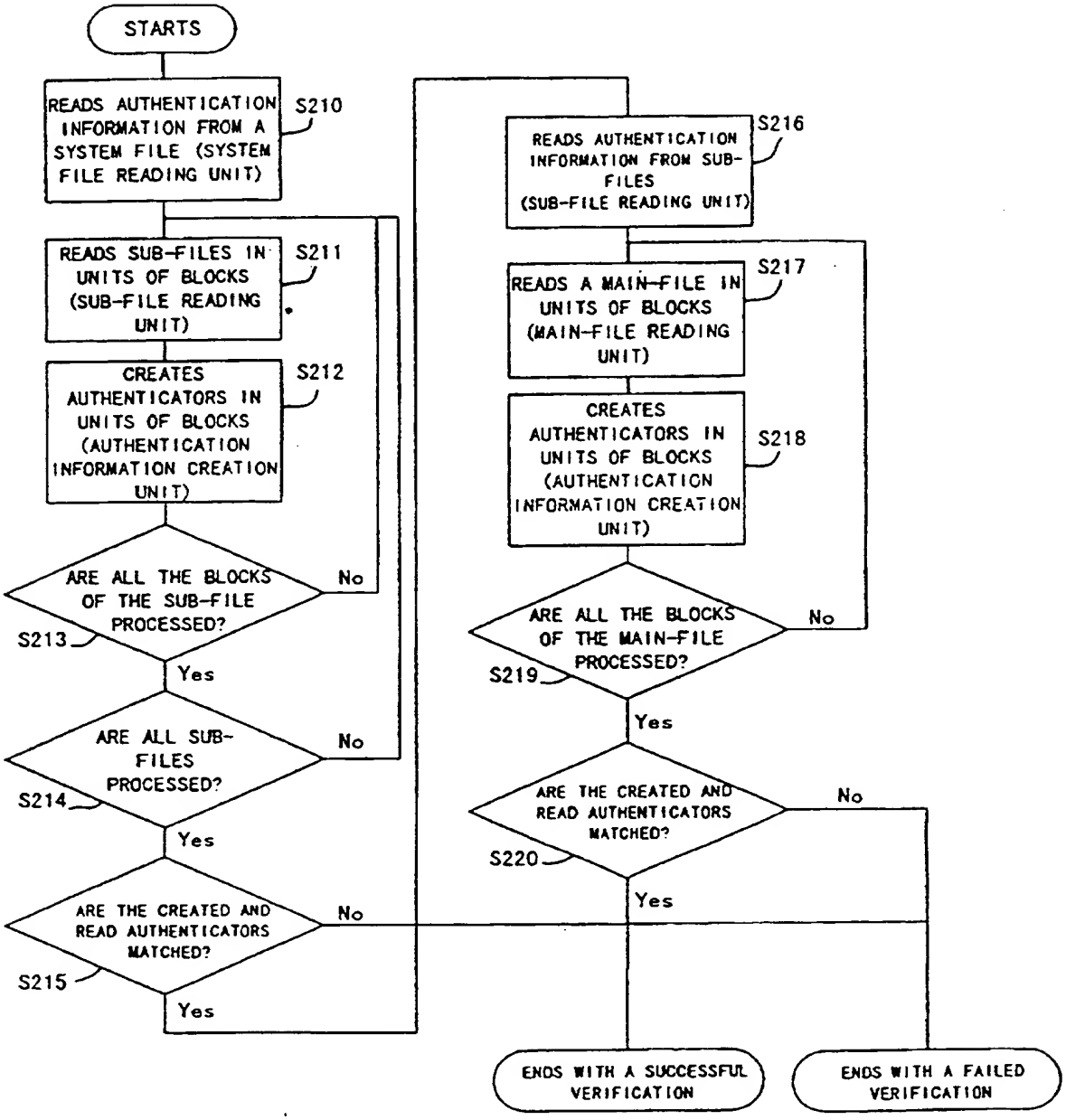

FIG. 21

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

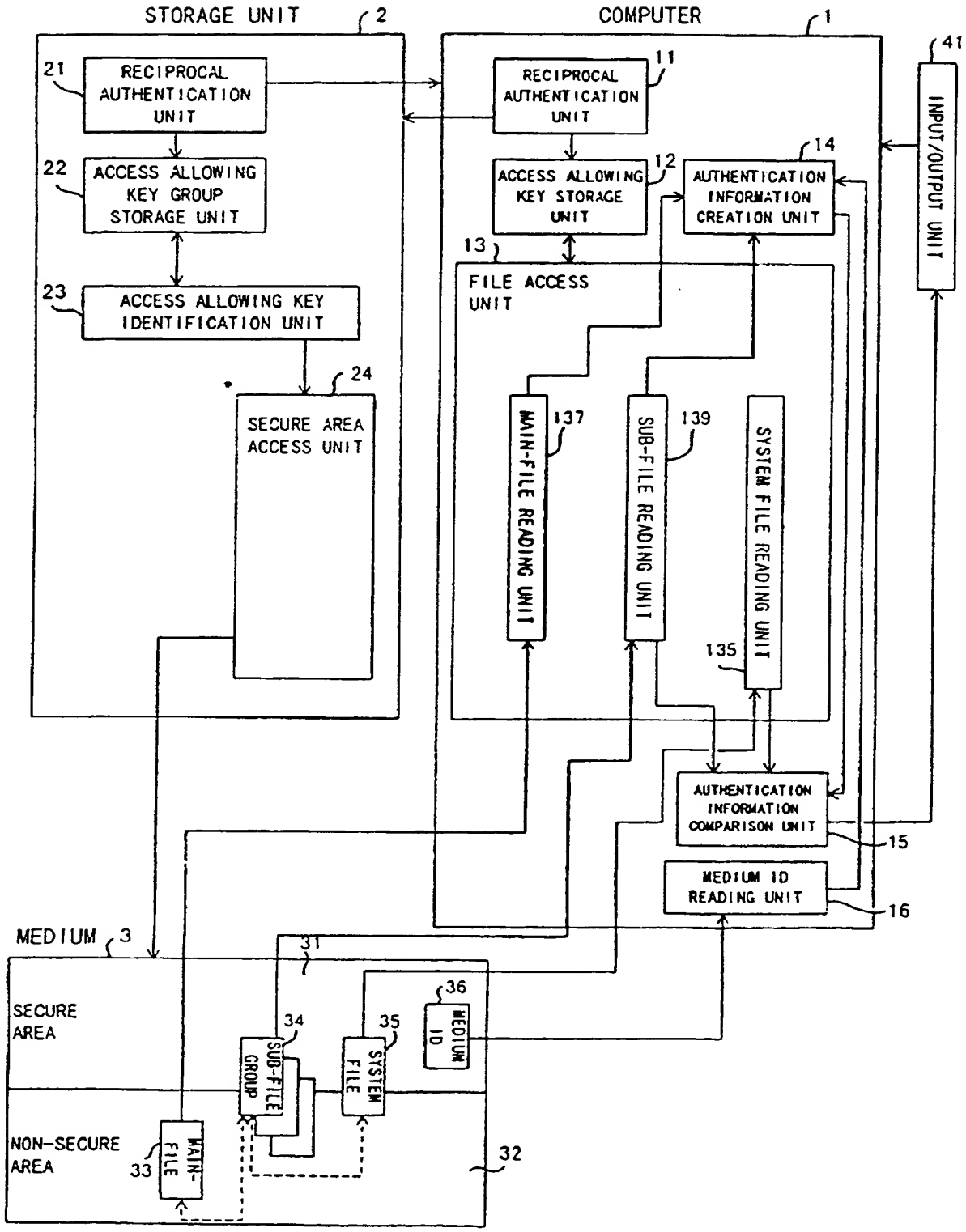

FIG. 22

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

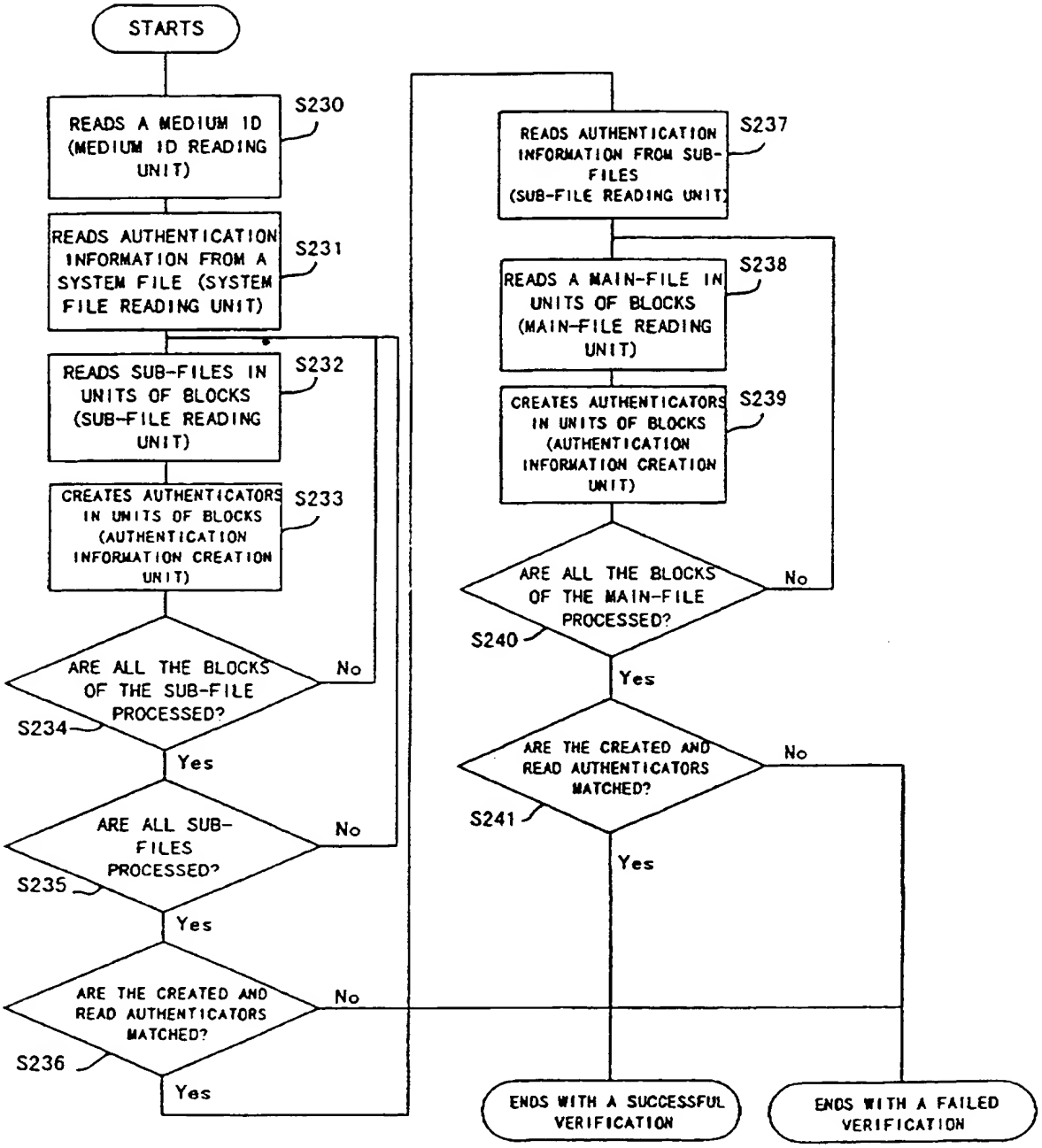

FIG. 23

BNSDOCID: <GB__2331381A__I_>
BNSDOCID: <GB 2331381A I >

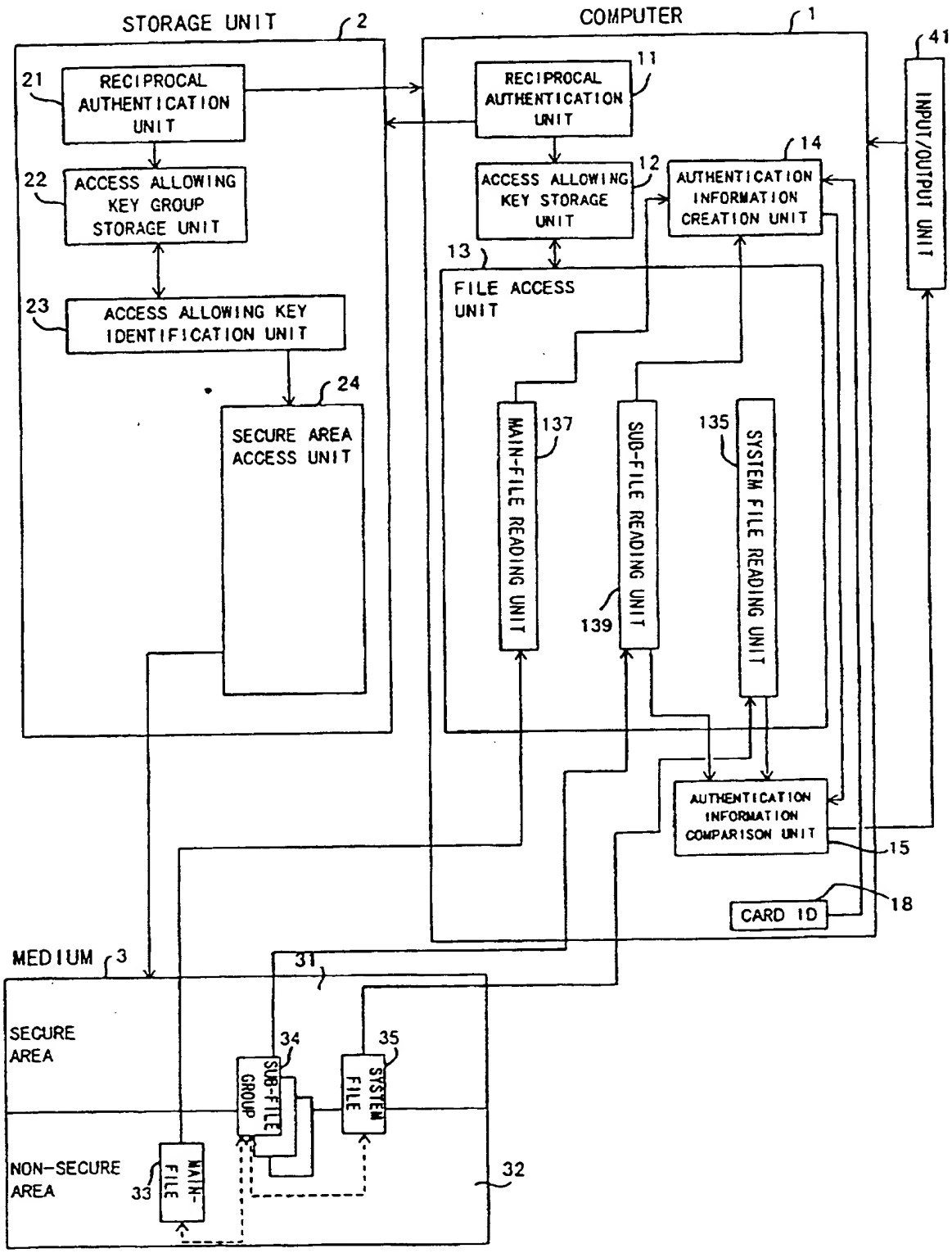

FIG. 24

BNSDOCID <GB___2331381A_I_>
BNSDOCID: <GB___2331381A_I_>

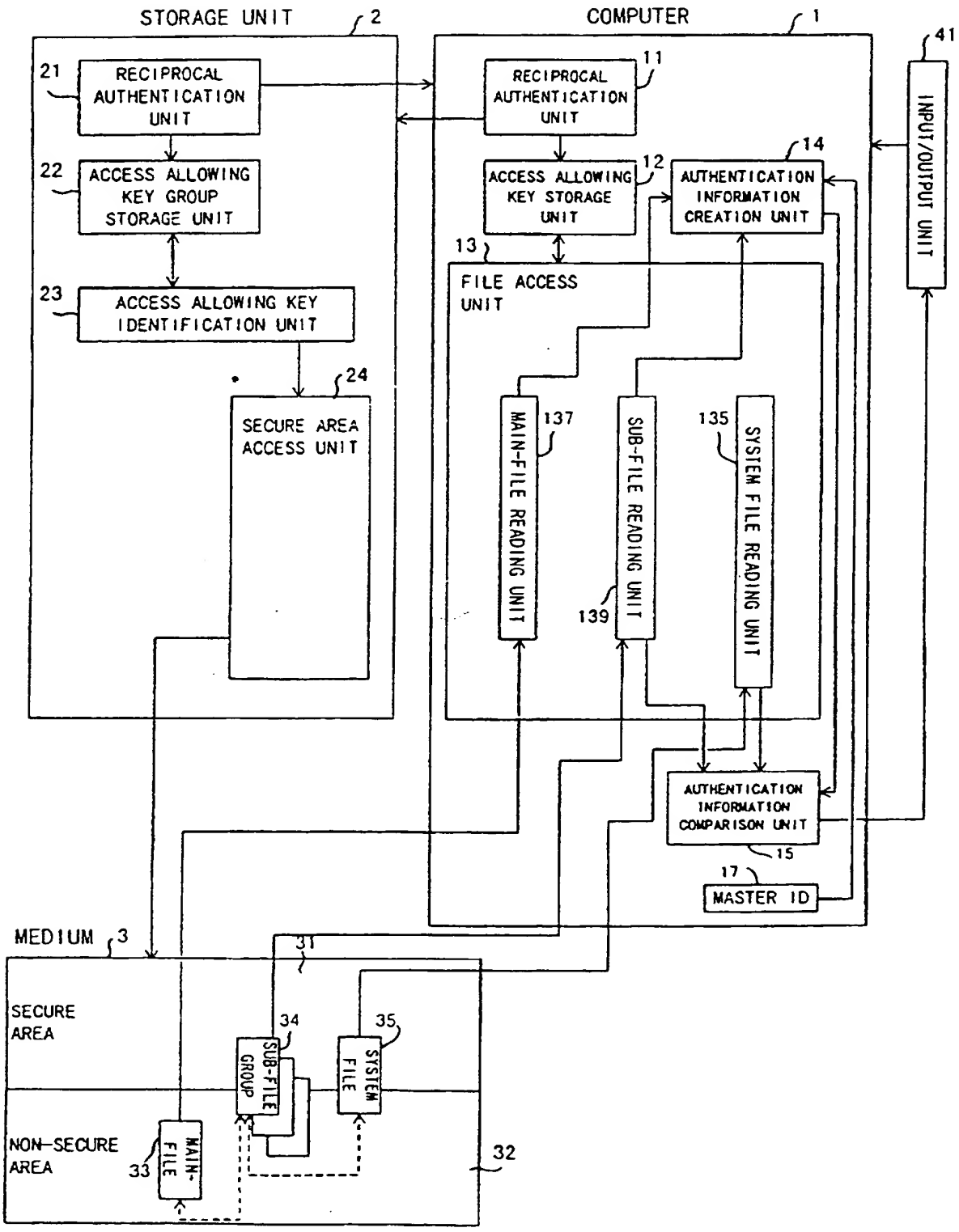

FIG. 25

BNSDOCID: <GB___2331381A__I_>
BNSDOCID: <GB___2331381A__I_>

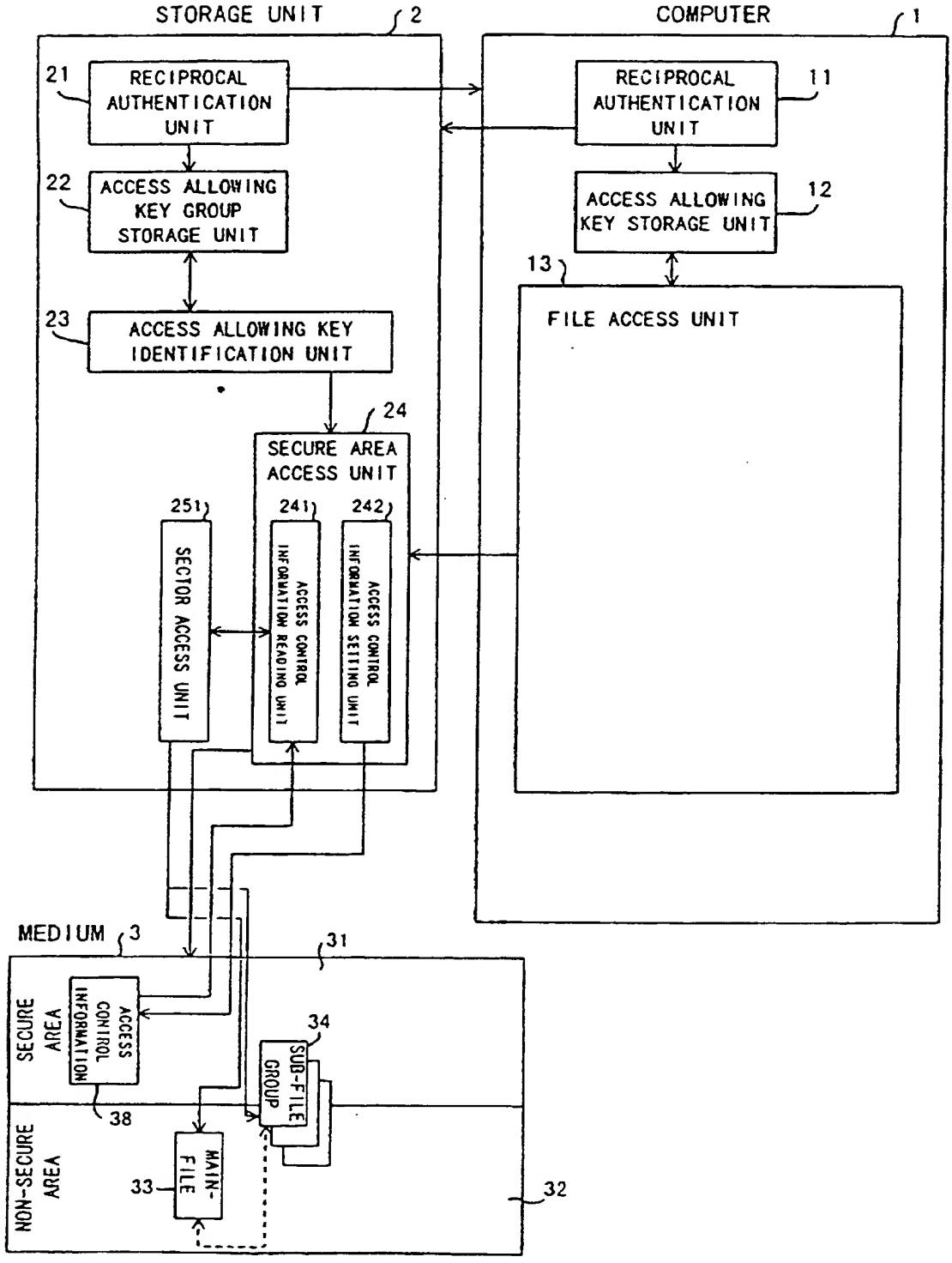

FIG. 26

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB___ 2331381A_I_>

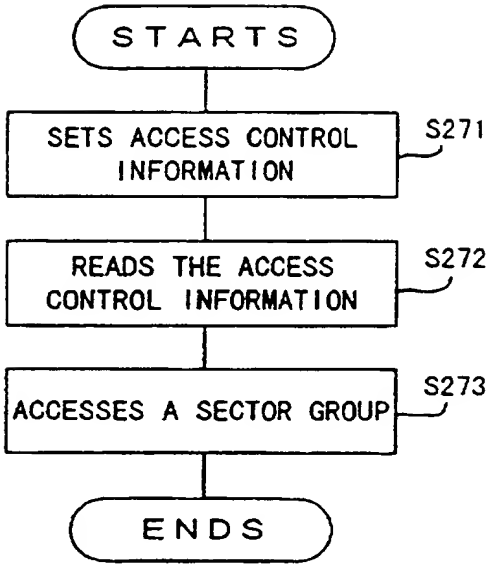

FIG. 27

BNSDOCID: <GB___2331381A__I_>

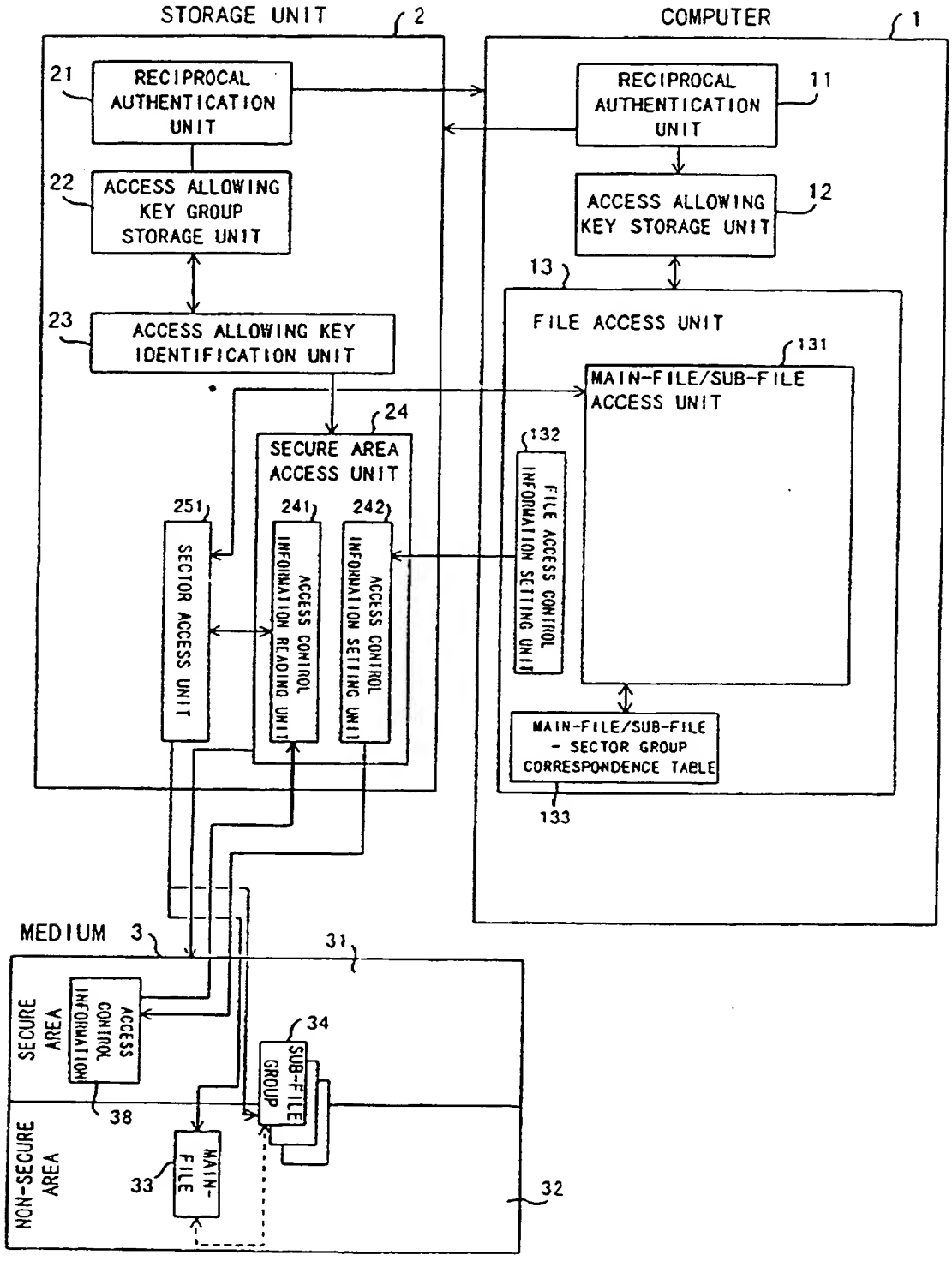

FIG. 28

BNSDOCID <GB___2331381A__I_>
BNSDOCID: <GB 2331381A I >

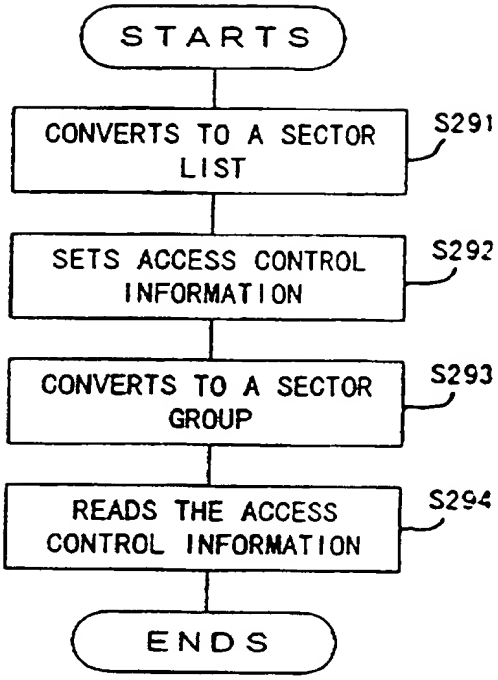

FIG. 29

BNSDOCID: <GB___2331381A_I_>
BNSDOCID: <GB 2331381A I >

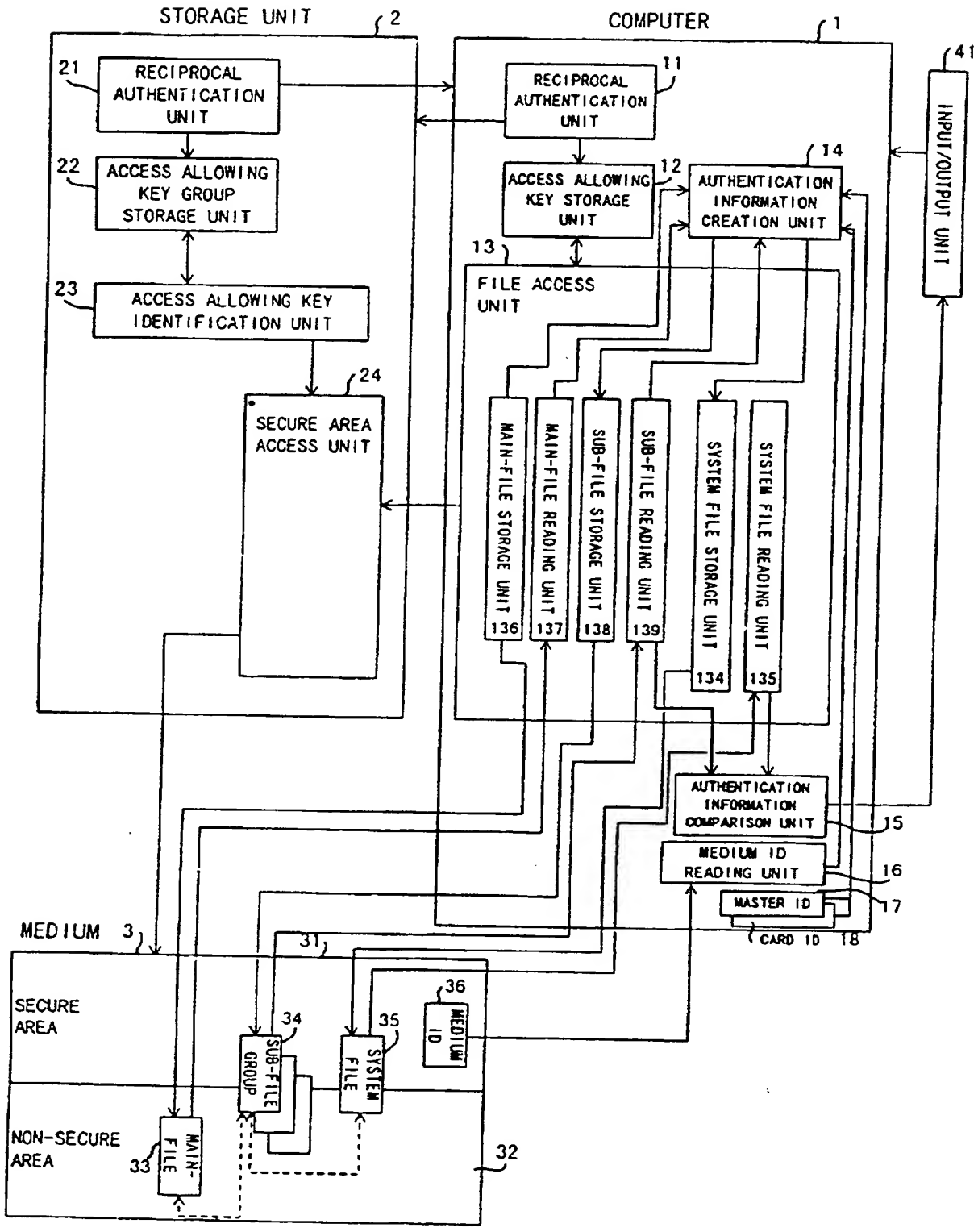

FIG. 30

BNSDOCID: <GB__2331381A_I_>
BNSDOCID: <GB__2331381A_I_>

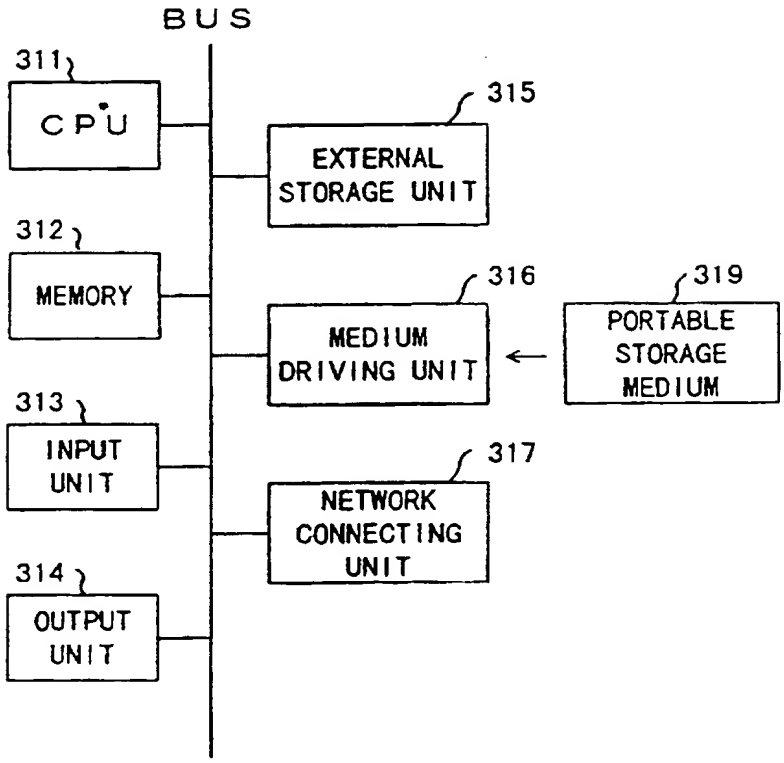

FIG. 31

BNSDOCID: <GB 2331381A_I_>
BNSDOCID: <GB 2331381A I >